ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン

(案)

総務省

平成 21 年○月

目次

第１章 本ガイドラインの前提条件及び読み方

本ガイドラインにおける記述の前提条件であるガイドラインの目的、本ガイドラインで想定する読者、本ガイドラインの読み方等を示す。なお本編を含め本ガイドラインで使用する用語については、１．６に示す。

１．１ 本ガイドラインの目的

１．１．１　医療情報の重要性とASP・SaaS利用の活用

（１） 医療情報に求められる高度なセキュリティ

一般に個人情報は、一旦漏洩等により流出した場合に回復措置が困難とされるものであるが、医療情報は個人の権利利益が侵害される可能性を孕むため、特に高い保護方策が求められる。そのため、医療機関等や関係者に対しては法律や各種のガイドライン等により格別の安全管理措置を講じることが求められている。

この様な経緯から、医療情報については医療機関等が自らの責任において管理し、医療情報を取り扱うシステムの導入時も、自らが管理するシステム等により行われてきた。

（２） 医療情報取扱におけるASP・SaaSの意義

しかしながら、情報処理システムの高度化、個人情報の保護やセキュリティに対する社会的な要請が高まる中、情報処理に係わる専門家ではない医療機関等や医療関係者がこれらの要請に耐えうることが困難な場面も見受けられるようになってきた。このような状況下においては、情報処理の専門家である情報処理事業者に管理責任を委ねる方が、安全性を確保できるケースが多いのも事実である。

他方、昨今は ASP・SaaS が普及し、様々な企業等の事業活動に活用されて来ている。この中には医療に係わる情報を処理する ASP・SaaS 事業者も見られ、これらの事業者に対する安全性確保の方策を検討する必要性も生じて来た。

今後、より一層 ASP・SaaS の利用が想定される中で、特に ASP・SaaS を活用して医療情報の処理を行う際には、高い安全性と効率化を実現する環境整備が期待されている。

１．１．２　本ガイドラインの目的

本ガイドラインでは、１．１．１に示す医療情報の重要性から見た高度な安全性の要求を踏まえ、ASP・SaaS 事業者が医療情報を取り扱う際に求められる責任等、ASP・SaaS 事業者への要求事項等、合意形成の考え方等を示す。本ガイドラインでは上記を通じて、医療情報が ASP・SaaS によって適正か

つ安全に利用され、医療情報における ASP・SaaS の利用の適切な促進を図ることを目的とする。

１．２ 本ガイドラインの対象範囲

本ガイドラインの対象範囲は、個人情報保護の観点から『医療・介護事業者における個人情報の適切な取扱いのためのガイドライン』（平成１６年１２月２４日（平成１８年４月２１日改正）厚生労働省）及びそこから参照することとされている「医療情報システムの安全管理に関するガイドライン第 4 版」（平成 21 年３月厚生労働省）（以下、「厚生労働省ガイドライン」という）において定義されているものと同一とする。

１．３ 対象とする事業者と他のガイドラインとの関係、ASP・SaaS提供に際しての前提事項

１．３．１　本ガイドラインで対象とする事業者等

本ガイドラインでは、医療情報の処理を ASP・SaaS で提供する事業者及び団体等を対象とする。但し医療情報の外部保存のみをサービスとして提供する者は含まない。

１．３．２　他のガイドラインとの関係

医療情報システムに関しては、厚生労働省から厚生労働省ガイドラインが示されている。これは医療情報システムを活用する際に、医療情報を安全に取り扱うのに必要な医療機関等の管理者の義務や責任、対応すべき内容等を示したものであり、ASP・SaaS により医療情報を処理する場合においても、医療機関等の管理者は、同ガイドラインの内容を踏まえることが求められる。

従って、ASP・SaaS により医療情報を処理する場合には、ASP・SaaS 事業者においても、この内容を前提として踏まえておかなくてはならない。

ASP・SaaS による医療情報の処理に関連するガイドラインの例として、厚生労働省ガイドラインのほかに、

① ASP・SaaS における情報セキュリティ対策ガイドライン（平成 20 年 1 月 30 日　総務省）(以下、「情報セキュリティ対策ガイドライン」という)

② 「医療情報を受託管理する情報処理事業者向けガイドライン」（平成 20 年 3 月 31 日　経済産業省）

等が挙げられる。

また１．１．１に示した医療情報の重要性に鑑みると、ASP・SaaS の対象とする医療情報の管理において、ASP・SaaS の情報セキュリティ対応は不可

欠であることから、先に示した①、②のガイドラインの内容も前提として考える必要がある。

本ガイドラインは、厚生労働省ガイドラインの内容をベースに、ASP・SaaS事業者の観点からの義務及び対応すべき事項を記述したものとして位置づける。

その際に、本ガイドラインは特に情報セキュリティ対策ガイドラインに記述されている安全対策を前提に捉えた上で、医療情報の重要性から強化すべき内容を記述している。

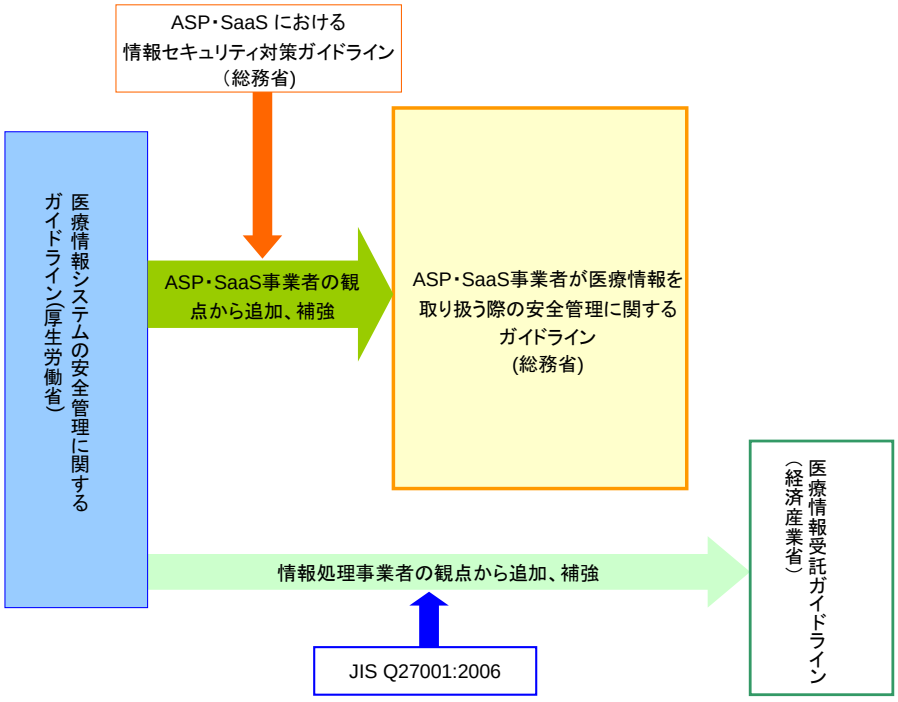

図　1-1　本ガイドラインと各ガイドラインの関係

1．3．3　ASP・SaaS提供に際して前提となる事項

（1）　医療情報を処理するすべてのASP・SaaS事業者における前提事項

1．3．2に示す通り、本ガイドラインは情報セキュリティ対策ガイドラインに加えて、医療情報の重要性等に鑑みて、必要な項目を追記している。従って ASP・SaaS の提供に際しては、情報セキュリティ対策ガイドライン及び本ガイドラインの遵守が必須である。

また、医療機関等に対して遵守していることを定期的に報告すること等も求められ、これらが ASP・SaaS 提供の前提事項となる。

但し ASP・SaaS のサービス提供がトランザクション型サービス（表1-1）など、外部保存を伴わない場合は、本ガイドライン 3.2 の外部保存

に関する対応内容を対象範囲に含めない等、本ガイドラインの遵守範囲を明らかにする必要がある。

医療情報を処理するすべての ASP・SaaS 事業者における、その他の前提事項として、以下の 3 点が挙げられる。

・守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わすこと。
・ネットワーク回線を含めて ASP・SaaS 事業者がサービスを提供する場合、そのネットワークの安全性に関しては、厚生労働省ガイドラインの「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守すること。
・契約に先立ち、医療機関等の管理者から、選定に必要な情報の提供を求められた場合に、速やかに提出すること。

（２） 外部保存を提供するサービスにおける前提事項

「『診療録等の保存を行う場所について」の一部改正について』（平成 17 年 3 月 31 日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長連名通知。以下「外部保存改正通知」という）で定められた文書の外部保存を、ASP・SaaS により行う際、（１）に加えて ASP・SaaS 事業者は以下内容を前提事項として行う必要がある。これらを実施する際の具体的な方法等については、ASP・SaaS 事業者と医療機関等で合意する必要がある（表 3-１５参照）。

・受託した医療情報を閲覧しないこと。ただし、保守等のために必要な場合は、その閲覧範囲を明確化して医療機関等に示すこと。
・受託した医療情報は、匿名化されたものを含めて分析、解析等を実施しないこと。ただし、医療機関等の委託がある場合は、実施範囲について委託契約等で明確にしておくこと。

１．４ 本ガイドラインで対象とするASP・SaaS

本ガイドラインにおいて適用対象とする ASP・SaaS と医療情報については、以下の通りである。

１．４．１ ASP・SaaSの定義

ASP（Application Service Provider）及び SaaS（Software as a Service）は、ともにネットワークを通じてアプリケーション・サービスを提供するものであり、基本的なビジネスモデルに大きな差はないものと考えられる。

したがって、本ガイドラインでは、ASP・SaaS インダストリ・コンソーシアム・ジャパンの発行した 2005 年版『ASP 白書』による ASP の定義『ネ

ットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること、あるいはそうしたサービスを提供するビジネスモデルを指す』を採用するとともに、ASP と SaaS を特に区別せず、「ASP・SaaS」と連ねて呼称することとする。また ASP・SaaS を行う事業者及び団体等を「ASP・SaaS 事業者」と呼ぶこととする（１．３．１参照）。

１．４．２　ASP・SaaSの分類

ASP・SaaS については、提供形態、利用形態の違いに着目して、分類することができる（表 1-1）。

表 1-1　ASP・SaaS の分類

分類の特徴	各分類の ASP・SaaS の特徴	
提供形態の特徴による区別	単独型	利用者に対して ASP・SaaS を、１事業者がすべて提供するもの。
	連携型	１事業者が利用者と契約を結び、他の複数の事業者のサービスを組み込んでサービス提供するもの。
利用形態の特徴による区別	単独利用	特定の ASP・SaaS を 1 利用者だけが利用する場合
	共同利用	特定の ASP・SaaS を複数の利用者が共同して利用する場合
外部保存に着目した区別	トランザクション型サービス	利用者から送信されたデータを ASP・SaaS で処理を行い、送信されたデータの保存は行わない。
	外部保存型サービス	利用者から送信されたデータを ASP・SaaS で処理を行うほか、送信されたデータの保存も行う。

１．５ 本ガイドラインの構成

本ガイドラインの構成を図 １-２に示す。

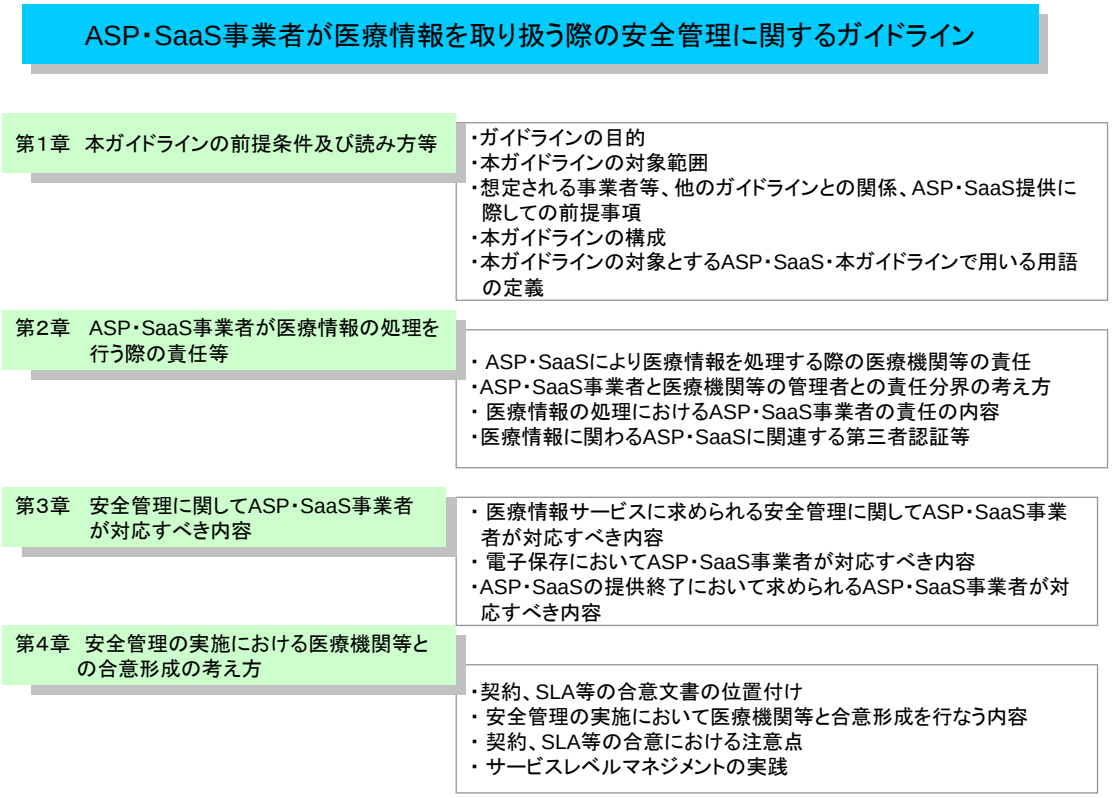

図 １-２ 本ガイドラインの構成

第 1 章では、本ガイドラインの対象となる ASP・SaaS 事業者や、具体的な対応をとる上で前提とすべき事項を整理した。

第 2 章では、ASP・SaaS 事業者の対応すべき内容の基礎となる責任や責任分界の考え方を整理した。

第 3 章では、医療機関等の管理者に対して求められる実施事項に関連する、ASP・SaaS 事業者への要求事項について示している。

第 4 章では、ASP・SaaS 事業者への要求事項のうち、医療機関等との合意形成が必要な場合の項目、考え方等を整理した。

１．６ 本ガイドラインで用いる用語の定義

１．６．１　厚生労働省ガイドラインで使用されている語の定義

厚生労働省ガイドラインで使用されている以下の用語については、「医療情報システムを安全に管理するために『医療情報システムの安全管理に関するガイドライン』すべての医療機関等の管理者向け読本」（厚生労働省、平成 21 年３月）から引用した。

i. 組織的安全管理対策

安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認することをいう。

ii.物理的安全対策

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

iii. 技術的安全対策

個人データ及びそれを取り扱う医療情報システムへのアクセス制御、不正ソフトウェア対策、医療情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

iv. 人的安全対策

従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

v.真正性

正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。

vi. 見読性

電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできることである。

ただし、見読性とは本来「診療に用いるのに支障が無いこと」と「監査等に差し支えないようにすること」であり、この両方を満たすことが、ガイドラインで求められる実質的な見読性の確保である。

vii. 保存性

記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されることをいう。

viii. 盗聴

ネットワークに特異な事象ではなく、広く一般的に、意図的に第三者が会話や情報を盗み聞いたり、盗み取る行為。ネットワークでは、一般的には何らかの手段で伝送中の情報（電気信号）を盗み取る行為を指す。

ix. 改ざん

情報を不正に書き換える行為のこと。例えば、ホームページを不正に書き換えたり、伝送途中の情報を書き換えたりする行為を指す。

x. なりすまし

本人ではない第三者が本人のふりをしてネットワーク上で活動すること。例えば、本来情報を受取る人のふりをして、不正に情報を取得する行為や他人の ID やパスワードを盗み出して、本人しか見ることができない情報を見たりする行為を指す。

１．６．２　情報セキュリティ対策ガイドラインにおける定義を踏襲している用語

情報セキュリティ対策ガイドラインで定義されている以下の用語については、情報セキュリティガイドラインの「Ｉ．９ 用語の定義」を踏襲する。

i.　機密性

認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。

ii.　完全性

資産の正確さ及び完全さを保護する特性。

iii. 可用性

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

iv. 情報資産

構成要素及び構成要素を介する情報

v.　情報セキュリティ

情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。

vi. リスク

事象の発生確率と事象の結果との組合せ。

vii. リスク分析

リスク因子を特定するための、及びリスクを算定するための情報の系統的使用。

viii. リスクアセスメント

リスク分析からリスク評価までのすべてのプロセス。

ix. 構成要素

ASP・SaaS サービスの提供に用いるハードウェア、ソフトウェア、通信機器・回線、建物等の固定資産。

x. 情報セキュリティポリシー

情報セキュリティに関する組織的取組についての基本的な方針及び情報セキュリティ対策における具体的な実施基準や手順等の総称。

xi. 利用者

ASP・SaaS サービスを利用する法人又は個人。

xii. 従業員

ASP・SaaS 事業者に所属し、当該 ASP・SaaS 事業者の提供する ASP・SaaS サービスの提供に携わる者で経営陣を除く者。派遣社員、アルバイト等を含む。

xiii. 管理責任者

ASP・SaaS サービスの提供に使用する設備の運用管理を担当する現場責任者。

xiv. 連携ASP・SaaS 事業者[1]

自らの ASP・SaaS サービスに他の ASP・SaaS サービスを組み込むことにより、アプリケーション間の統合・連携を実施する際に、他の ASP・SaaS サービスを提供する ASP・SaaS 事業者。

xv. 外部組織[2]

連携 ASP・SaaS 事業者や ASP・SaaS 事業者からサービスの一部を委託された企業等、ASP・SaaS サービスの提供にあたり契約関係のある組織の総称。

xvi. 業務プロセス

ASP・SaaS サービスを提供するために行われる一連の活動。

xvii. ユーザサポート

ASP・SaaS サービスに関する問い合わせ窓口（ヘルプデスク）と ASP・SaaS サービスの品質や継続性を維持するための組織の総称。

xviii. 情報処理施設

ASP・SaaS 事業者がサービスを提供するための設備が設置された建物。

xix. 物理的セキュリティ境界

---

[1] 本ガイドラインにおける「連携 ASP・SaaS 事業者」は、ASP・SaaS 事業者からの委託契約等に基づいて、医療機関等に ASP・SaaS を提供を行う事業者をいう。

[2] 本ガイドラインで「外部組織」には、連携 ASP・SaaS 事業者に加え、サービスを提供する ASP・SaaS 事業者から委託を受けて、サービスの一部やサービス提供に必要な保守業務等の業務を行う者を含む。

情報処理施設の特定の領域を保護するために設置される壁、カード制御による出入口等の物理的な仕切り。

xx. サーバ・ストレージ

ASP・SaaS サービスを提供する際に利用するアプリケーション等を搭載する機器及びアプリケーション上の情報を蓄積・保存するための装置の総称。なお、付随する OS 等の基盤ソフトウェア、蓄積されているデータ・ログ等の情報を含む。

xxi. プラットフォーム

認証、決済等の付加的機能を提供する、ASP・SaaS サービスで提供されるアプリケーションの基盤。

xxii. 通信機器

ルータ、スイッチ等、通信を制御するための装置。

xxiii. 情報セキュリティ対策機器

ファイアウォール、IDS 等、コンピュータウイルスや不正アクセス等の情報セキュリティ事象から、ASP・SaaS 事業者の設備を防護するための機器。

xxiv. 外部ネットワーク

情報処理施設とその外部とを結ぶネットワークの総称で、ASP・SaaS 事業者と ISP 間、ASP・SaaS 事業者と連携 ASP・SaaS 事業者間、ASP・SaaS 事業者の保守管理用回線等を指す。本ガイドラインの対象外である、利用者が契約する通信回線及びインターネット・サービスは除く。

１．６．３　本ガイドラインで定義する用語

本ガイドラインで定義する用語は以下の通りである。

i. SLA

ASP・SaaS における SLA(Service Level Agreement）とは、サービス提供事業者とサービス利用者が ASP・SaaS の利用契約を締結するにあたり、両者がサービス及びサービスレベルについて合意した内容を明文化したものである。

第２章　ASP・SaaS事業者が医療情報の処理を行う際の責任等

本章ではASP・SaaS事業者が医療情報の処理を行うにあたって、医療機関等に求められる責任等を踏まえた上で、ASP・SaaS事業者が分担する責任と責任分界の考え方をまとめる。

２．１ 医療情報を処理する際の医療機関等の責任

【「医療機関等の管理者の責任」に関する記述】（厚生労働省ガイドライン）（図２-１参照）

【医療機関等の管理者の責任】

・「医療に関わるすべての行為は医療法等で医療機関等の管理者の責任で行うことが求められており、医療情報の取扱いも同様である。」（「4 電子的な医療情報を扱う際の責任のあり方」）

【医療機関等の管理者の責任の種類】

・「医療機関等の管理者が医療情報を適切に管理するための善管注意義務を果たすためには、通常の運用時から払われているべき、医療情報保護の体制を構築し管理する局面での責任と、医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合に対処をすべき責任とがある。便宜上、本ガイドラインでは前者を「通常運用における責任」、後者を「事後責任」と呼ぶこととする。」（「4.1 医療機関等の管理者の情報保護責任について」）

【通常運用における責任】

・「ここでいう通常運用における責任とは、医療情報の適切な保護のための適切な情報管理ということになるが、適切な情報管理を行うことが全てではなく、以下に示す3つの責任を含む必要がある。」（4.1(1) 通常運用における責任について」）

【事後責任】

・「医療情報について何らかの不都合な事態（典型的には漏えい）が生じた場合には、以下の責任がある。」（4.1（2） 「事後責任について」）

図　2-1　医療機関等の管理者が電子的な医療情報を扱う際の責任の構成

２．２ ASP・SaaS事業者と医療機関等の管理者との責任分界の考え方

厚生労働省ガイドラインでは、２．１で示すように、医療情報を電子的な形で取り扱う場合、医療機関等の管理者がこれに関連する責任を負うとする。しかしながら、医療機関等が ASP・SaaS 等で医療情報を取り扱うサービスを利用する場合、医療機関等との契約に基づいて ASP・SaaS 事業者等の情報処理事業者がシステムやデータの管理等を行う。この場合、医療情報を電子的に取り扱う際の責任を、医療機関等の管理者と ASP・SaaS 事業者とで分担することが必要となる。分担するためには、医療機関等の管理者と ASP・SaaS 事業者が以下の内容を明らかにする必要がある。

・提供する ASP・SaaS における医療機関等と ASP・SaaS 事業者との責任分界
・ASP・SaaS 事業者が提供するサービスの内容及びレベルの具体化

また責任分界を定める前提として、ASP・SaaS による医療情報の処理に伴い医療機関等の管理者が対応すべき事項等を整理する必要がある。その際、ASP・SaaS 事業者は対応すべき内容を定める際に基本的な姿勢として、情報システムの安全管理に係る高いノウハウを基に、専門的な見地からの助言等を医療機関等の管理者に対して責任を持って行うことが必要である。

２．３ 医療情報の処理におけるASP・SaaS事業者の責任

医療機関等で医療情報を ASP・SaaS を活用して処理する場合には、これらの医療機関等の管理者が負う責任の一部を、ASP・SaaS 事業者が分担する。

例えば ASP・SaaS を支えるシステムの仕様や運用、サービスの品質管理やそれらに対する定期的な監査等については、ASP・SaaS 事業者が直接的な管理をしており、ASP・SaaS 事業者はこれらの部分について、医療機関等の管理者に課される責任を委託契約により分担することになる。

２．３．１　通常運用における責任

医療機関等の管理者が患者等に対して負う「通常運用における責任」については、厚生労働省ガイドラインの 4.1 に記述されている。「通常運用における責任」には、「説明責任」、「管理責任」、「定期的に見直し必要に応じて改善を行う責任」がある。

以下、医療機関等の管理者の負う責任を踏まえて、通常運用における責任に含まれる各責任のうち、ASP・SaaS 事業者が負う責任の内容を整理する（具体的な実施内容については、第３章に示す ASP・SaaS 事業者への要求事項を参照）。

（１） 通常運用における責任の説明責任

① 厚生労働省ガイドラインの記述

通常運用における責任の説明責任に関する医療機関等の管理者の情報保護責任及び委託における責任分界についての厚生労働省ガイドラインの記述を以下に示す（()内の数字は厚生労働省ガイドラインの記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(1)①)

電子的に医療情報を取り扱うシステムの機能や運用計画が、その取り扱いに関する基準を満たしていることを患者等に説明する責任である。これを果たすためには、以下のことが必要である。

- システムの仕様や運用計画を明確に文書化すること
- 仕様や計画が当初の方針の通りに機能しているかどうかを定期的に監査すること
- 監査結果をあいまいさのない形で文書化すること
- 監査の結果問題があった場合は、真摯に対応すること
- 対応の記録を文書化し、第三者が検証可能な状況にすること

【委託における責任分界】（4.2.1(1)①）

患者等に対し、いかなる内容の医療情報保護の仕組みが構築されどのように機能しているかの説明責任は、いうまでもなく医療機関等の管理者にある。

ただし、医療機関等の管理者が説明責任を果たすためには、受託する事業者による情報提供が不可欠の場合があり、受託する事業者は医療機関等の管理者に対し説明責任を負うといってよい。 従って、受託する事業者に対し適切な情報提供義務・説明義務を委託契約事項に含め、その履行を確保しておく必要がある。

② ASP・SaaS事業者が負う「通常運用における責任」の「説明責任」

医療機関等の管理者に課せられる「電子的に医療情報を取り扱うシステムの機能や運用計画が、その取り扱いに関する基準を満たしていることを患者等に説明する責任」を果たすために、ASP・SaaS 事業者は以下の責任を負わなくてはならない。

- 提供サービスの仕様及び運用、セキュリティ対策に関する文書化
- 提供するサービスの仕様及び提供する品質に関する説明及び必要な情報提供
- サービス提供に関する監査等情報提供

（２） 通常運用における責任の管理責任

① 厚生労働省ガイドラインの記述

通常運用における責任の管理責任に関する医療機関等の管理者の情報保護責任及び委託における責任分界についての厚生労働省ガイドラインの記述を以下に示す（()内の数字は厚生労働省ガイドラインの記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(1)②)

医療情報を取り扱うシステムの運用管理を行う責任であり、当該システムの管理を請負事業者に任せきりにしているだけでは、これを果たしたことにはならないため、医療機関等においては、以下のことが必要である。

・少なくとも管理状況の報告を定期的に受けること
・管理に関する最終的な責任の所在を明確にする等の監督を行うこと

さらに、個人情報保護法上は、以下の事項を定め、請負事業者との対応にあたる必要がある。

・個人情報保護の責任者を定めること
・電子化された個人情報の保護について一定の知識を有する責任者を決めること

【委託における責任分界】（4.2.1(1)②）

管理責任を負う主体はやはり医療機関等の管理者にある。しかし、現実に情報処理に当たりその安全な保守作業等を行うのは、委託先事業者である場面が多いと考えられる。医療機関等の管理者としては、委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る必要があり、契約事項に含めるべきである。

② ASP・SaaS事業者が負う「通常運用における責任」の「管理責任」

医療機関等の管理者に課せられる「医療情報を取り扱うシステムの運用管理を、行う責任」を果たすために、ASP・SaaS 事業者は以下の責任を負わなくてはならない。

・医療機関等の管理者に対する最終的な管理責任者の明確化
・個人情報保護管理を含むサービス提供体制の明確化
・サービス提供に関する運用等の定期的な報告
・医療機関等の管理者からの問合せ等に対して、一元的に対応できる体制の構築

（３） 通常運用における責任の定期的に見直し必要に応じて改善を行う責任

① 厚生労働省ガイドラインの記述

通常運用における責任の定期的に見直し必要に応じて改善を行う責任に関する医療機関等の管理者の情報保護責任、及び委託における責任分界についての厚生労働省ガイドラインの記述を以下に示す（()内の数字は厚生労働省ガイドラインの記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(1)③)

・情報保護に関する技術は日進月歩であるため、情報保護体制が陳腐化する恐れがあり、それを適宜見直して改善するためには以下の責任を果たさなくてはならない。

・当該情報システムの運用管理の状況を定期的に監査すること

・問題点を洗い出し、改善すべき点があれば改善すること

そのために医療機関等の管理者は、医療情報保護の仕組みの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行う必要がある。

【委託における責任分界】（4.2.1(1)③）

当該システムの運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していく責任の分担、また、情報保護に関する技術進展に配慮した定期的な再評価・再検討について委託先事業者との契約事項に含めるべきである。

② ASP・SaaS事業者が負う通常運用における責任の定期的に見直し必要に応じて改善を行う責任

医療機関等の管理者に課せられる、情報保護体制が陳腐化するのを防止し、それを適宜見直して改善する責任を果たすために、ASP・SaaS 事業者は以下の責任を負わなければならない。

・サービス提供改善及びセキュリティ向上の必要性についての定期的なレビュー結果の報告

２．３．２　事後責任

医療機関等の管理者が患者等に対して負う事後責任については、厚生労働省ガイドラインの 4.1 に記述されている。事後責任には、説明責任、善後策を講じる責任がある。

以下、医療機関等の管理者の負う責任を踏まえて、事後責任に含まれる各責任のうち、ASP・SaaS 事業者の負う責任の内容を整理する（具体的な実施内容については、第３章に示す ASP・SaaS 事業者への要求事項を参照)。

（１） 事後責任における説明責任

① 厚生労働省のガイドラインの記述

事後責任の説明責任に関する医療機関等の管理者の情報保護責任、及び委託における責任分界についての厚生労働省ガイドラインの記述を以下に示す（()内の数字は厚生労働省ガイドラインの記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(2)①)

特に医療機関等は一定の公共性を有するため、個々の患者に対する説明責任があることは当然ながら、併せて監督機関である行政機関や社会への説明・公表も求められる。そのため、以下のことが必要である。

・医療機関等の管理者はその事態発生を公表すること

・原因といかなる対処法をとるかについて説明すること。

【委託における責任分界】（4.2.1(2)①）

前項で述べたように、医療情報について何らかの不都合な事態が生じた場合、医療機関等の管理者にはその事態発生を公表し、その原因といかなる対処法をとるかについて説明する責任が求められている。 しかし、情報に関する事故は、説明に際して受託する事業者の情報提供や分析が不可欠な場合が多いと考えられる。そのため予め可能な限りの事態を予想し、受託する事業者との間で、説明責任についての分担を契約事項に含めるべきである。

② ASP・SaaS事業者が負う事後責任の説明責任

医療機関等の管理者に課せられる、「個々の患者に対する説明責任」及び「監督機関である行政機関や社会への説明・公表」の責任を果たすために、ASP・SaaS 事業者は以下の責任を負わなければならない。

・緊急時における医療機関の管理者に対して提供する情報内容、役割分担等の明確化

・サービス提供状況に関する記録を収集、緊急時の報告体制の構築

・媒体管理及び機器の管理等に関する手順の明確化及び緊急時の報告体制の構築

・緊急時に備えたアクセス制御等の手順等の明確化

（２） 事後責任における善後策を講ずる責任

① 医療機関等の管理者の責任

事後責任の説明責任に関する医療機関等の管理者の情報保護責任、及び委託における責任分界についての厚生労働省ガイドラインの記述を以下に示す（()内の数字は厚生労働省ガイドラインの記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(2)②)

医療機関等の管理者には善後策を講ずる責任も発生する。その責任は以下に分けられる。

１）原因を追及し明らかにする責任

２）損害を生じさせた場合にはその損害填補責任

３）再発防止策を講ずる責任。

【委託における責任分界】（4.2.1(2)②）

事故が医療情報の処理を委託した事業者の責任による場合、適切な委託契約に基づき、受託する事業者の選任・監督に適切な注意を払っていれば、法律上、医療機関等の管理者の善管注意義務は果たされていると解される。

とはいえ、本章冒頭に述べたように、医療機関等では医療情報の管理を医療機関等の管理者の責任において行うことが求められているので、医療情報に関する事故の原因究明、被害者への損害填補、さらに再発防止について、少なくとも責任の一端を負わなければならない。また、現実的にも、受託する事業者が医療情報のすべてを管理しているとは限らないため、事故を契機として、医療情報保護の仕組み全体について善後策を講ずる責任は医療機関等の管理者が負わざるを得ない。

医療機関等の管理者は、患者に対して、１）原因を追及し明らかにする責任、２）損害を生じさせた場合にはその損害填補責任、３）再発防止策を講ずる責任、の善後策を講ずる責任を免れるものではない。

医療機関等の管理者の、患者等に対するすべての責任が免ぜられることはないとしても、受託する事業者との間での責任分担はそれとは別の問題であり、特に、事故が受託する事業者の責任で生じた場合、医療機関等の管理者がすべての責任を負うことは、原則としてあり得ない。

しかし医療情報について何らかの事故が生じた場合、医療機関等と受託する事業者の間で責任の分担について争うことに優先して、まず原因を追及し明らかにすること、そして再発防止策を講ずることが重要である。

委託契約に、医療機関等と受託する事業者が協力してこれらの措置を優先させることを明記しておく必要がある。

委託内容によっては、より詳しく受託する事業者の責任での原因追及と再発防止策の提案義務を明記することも考えられる。

損害填補責任の分担については、事故の原因が受託する事業者にある場合、最終的には受託する事業者が負うのが原則である。ただし、この点は、原因の種類や複雑さによっては原因究明が困難になること、また損害填補責任分担の定め方によっては原因究明の妨げになるおそれがあること、あるいは保険による損害分散の可能性など、さまざまに考慮すべき要素があり、それらを考慮した上で、委託契約において損害填補責任の分担を明記することが必要である。

② ASP・SaaS事業者が負う事後責任の善後策を講ずる責任

医療機関等の管理者に課せられる「１）原因を追及し明らかにする責任」、「２）損害を生じさせた場合にはその損害填補責任」、「３）再発防止策を講ずる責任」を果たすために、ASP・SaaS 事業者は以下の責任を負わなければならない。

・情報事故等が発生した場合の原因追及に必要な情報の提供の範囲、条件等の合意、及びその実施
・善後策として講じる対応策等の提案
・情報事故が発生した場合の損害賠償責任に関する合意

２．４ 医療情報に関わるASP・SaaS事業者に関連する第三者認証等の考え方

ASP・SaaS により医療情報を処理する場合に、第三者認証等を取得して、マネジメントシステムの上で運用することは、医療機関等の管理者が管理責任や説明責任を果たす際、システムや運用状況を客観的に把握できるようにするため、非常に有効な手段であると考えられる。

医療情報の処理に当たっては、個人情報の取り扱いについて、特に高い注意義務を要することから、ASP・SaaS 事業者においては、プライバシーマークを取得することが強く求められる。また不足なく適用範囲を定めた適用宣言書に基づく ISMS 認定の取得を考慮することも求められる。

第３章 安全管理に関してASP・SaaS事業者への要求事項

本章では、ASP・SaaS 事業者がサービス提供に際して対応すべき内容を記述する。医療情報サービスに求められる安全管理に関する実施項目については、厚生労働省ガイドライン「6 情報システムの基本的な安全管理」で記述されている。

３．１ 本章の読み方

３．１．１ ASP・SaaS事業者が実施すべき内容

３．２では、すべての ASP・SaaS 事業者への要求事項を記述する。

３．３では、ASP・SaaS により、医療機関等から外部保存改正通知に基づいて医療情報の外部保存を受託する ASP・SaaS 事業者への要求事項について記述する（図 ３-１参照)。

３．４では、ASP・SaaS の提供が終了する場合の ASP・SaaS 事業者への要求事項について記述する。

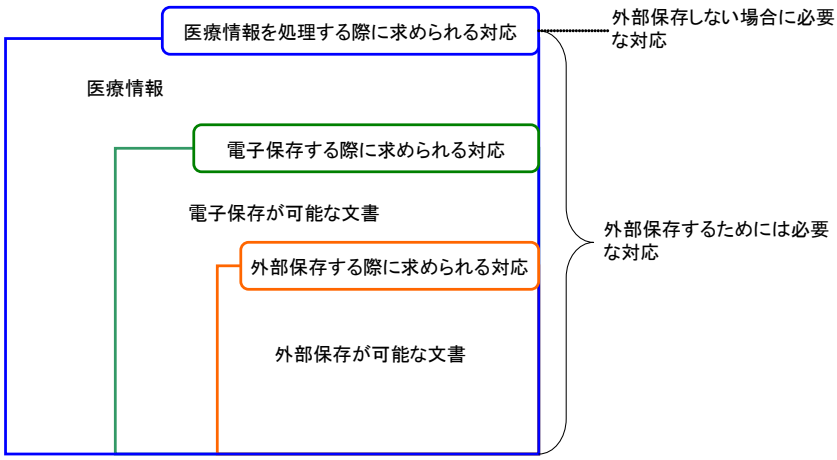

図 ３-１ 各医療情報等に対する ASP・SaaS 事業者の対応

３．１．２ 本章で記述する表の見方

（１） 各項目の記述内容

本章３．２以下では、ASP・SaaS 事業者への要求事項を表形式で下記のように整理した（図 ３-２)。

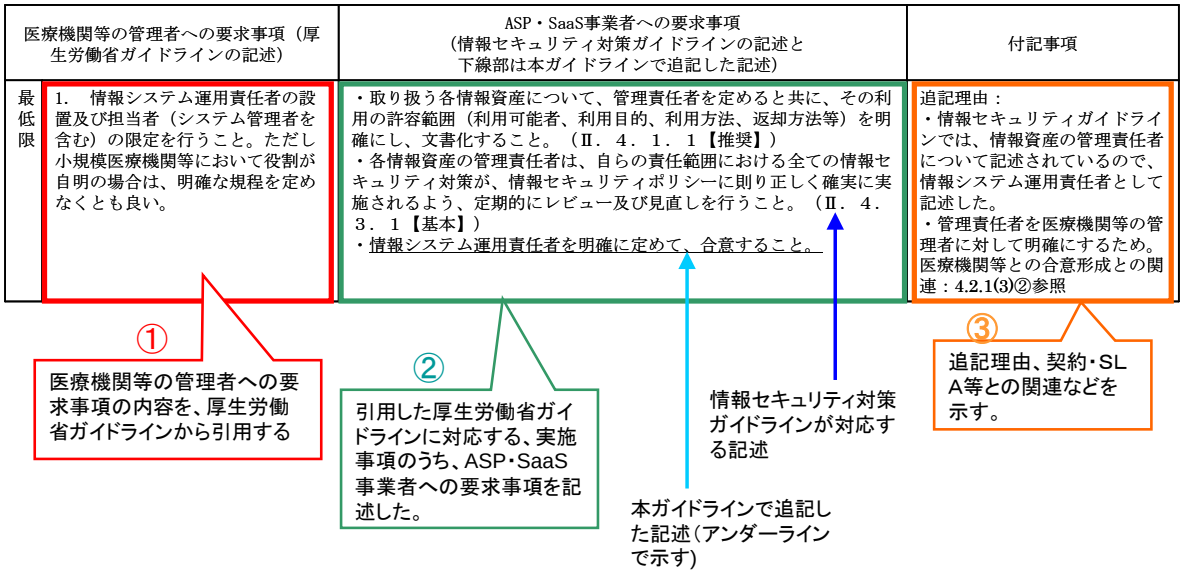

図 3-2 第 3 章の各表の見方

① 医療機関等の管理者の要求事項

医療機関等の管理者が行うべき内容を、厚生労働省ガイドラインから示す。

② ASP・SaaS 事業者への要求事項

・情報セキュリティ対策ガイドラインの記述

引用した厚生労働省ガイドラインに対応する実施事項のうち、情報セキュリティ対策ガイドラインで【基本】として記述されている内容を示す。

・本ガイドラインで追記した内容

医療情報の重要性等から、本ガイドラインで追記した内容を示す。

③ 付記事項

情報セキュリティ対策ガイドラインに追記した理由、第 4 章における医療機関等との合意形成に関連する箇所を示した。

厚生労働省ガイドライン及び情報セキュリティ対策ガイドラインの記述内容についてご理解を頂いている方については、（図 3-2）の「ASP・SaaS 事業者の対応すべき内容」を中心にお読み頂きたい。

（２） ASP・SaaS事業者への要求事項の見方

本章で示す各表中の「ASP・SaaS事業者への要求事項」のうち、情報セキュリティ対策ガイドラインの対策項目[3] は、サービス提供にあたって優先的に実施すべき内容であり、医療機関等においても基本的に「対策済み」であることを前提とする。従って、ASP・SaaS事業者は、これらの項目が

[3] 正確には「基本」に分類される対策項目がこれにあたる。

「対策済み」であることを医療機関等に確認した上でサービスを提供しなくてはならない。また情報セキュリティ対策ガイドラインにおいて【推奨】としている内容についても、厚生労働省ガイドラインにおいて「最低限」となっている項目については、必須対応事項とする。

本ガイドラインで、医療情報サービスの提供に特化して追記された内容については、医療機関等が求める責任分担やサービスレベルにかなり幅があるものが含まれており、具体的な内容については、医療機関等との合意が必要であるものがある。このような内容については、「医療機関等と合意すること」、と記述した。なお医療機関等との合意内容については、情報セキュリティ対策ガイドライン及び本ガイドラインの内容を満たすものであることが求められる。

３．２ 医療情報サービスに求められる安全管理に関するASP・SaaS事業者への要求事項

以下では、情報システムの安全性のために、医療機関等の管理者に対する要求事項とされているものに対して、これに呼応する形で、ASP・SaaS 事業者への要求事項を整理する。

ASP・SaaS 事業者は対応すべき内容を定める際に基本的な姿勢として、情報システムの安全管理に係る高いノウハウを基に、専門的な見地からの助言等を医療機関等の管理者に対して責任を持って行うことが必要である。

３．２．１　組織的安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、組織的安全管理対策について、第 6 章 6.3 に記述している。

（２） ASP・SaaS事業者への要求事項

組織的安全管理対策における ASP・SaaS 事業者への要求事項について表３-１に整理する。

表 3-1　組織的安全管理対策における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【推奨】） ・各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。（Ⅱ．４．３．１【基本】） ・情報システム運用責任者を明確に定めて、合意すること。	追記理由： ・情報セキュリティガイドラインでは、情報資産の管理責任者について記述されているので、情報システム運用責任者として記述した。 ・管理責任者を医療機関等の管理者に対して明確にするため。 医療機関等との合意形成との関連：4.2.1(3)②参照
最低限	2.　個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．４．４．１【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅲ．４．４．３【基本】） ・受託した個人情報を参照可能な事務室等における入退室管理のルールが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・事務室等の入退出について追記したため。 ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(4)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	3.　情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。	・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．５．３．１【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。　また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。　また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・運用しているアクセス管理に関する規程類が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・自社の規程類の情報を医療機関に対して開示する範囲・条件等について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 ・アクセス管理規程等は、セキュリティ上、事業者の秘密にあたる場合があるので、開示の範囲、条件等を定めるため。 医療機関等との合意形成との関連：4.2.1(4)、(5)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）			ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。		・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・自社で定める個人情報保護指針等に基づいて、委託業務を実施する旨を、契約内容に含めること。 ・自社で定める個人情報保護指針等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000 件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・個人情報保護指針等による旨を契約に含めるため。 ・医療機関等の定める規程等との内容との整合性をとるため。 ・医療情報の重要性からの取り扱いが必要なため。 医療機関等との合意形成との関連：4.2.1(2)②、(4)参照
最低限	5. 運用管理規程等において次の内容を定めること。			
		(a) 理念（基本方針と管理目的の表明）	・経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。（Ⅱ．１．１．１【基本】） ・自社で定める情報セキュリティに関する組織的取組における基本方針が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(3))参照
		(b) 医療機関等の体制	・医療機関等の体制に対応する事業者の体制を明らかにすることを、医療機関等と合意すること。	補足理由： ・医療機関の体制に対応する事業者側の体制を明確にするため。 医療機関等との合意形成との関連：4.2.1(3)①参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）			ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
		(c) 契約書・マニュアル等の文書の管理	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・マニュアル等の文書管理に関して、開示できる文書等の範囲、事業者の役割等を医療機関等と合意すること。	追記理由： ・ニュアル等の文書管理に関して、開示内容を合意を含めるため。 医療機関等との合意形成との関連：4.2.1(4)参照
		(d) リスクに対する予防、発生時の対応の方法	・全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。 報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。（Ⅱ．６．１．１【基本】） ・自社で定めるリスク等に対する予防措置及び事故等の発生時の対応等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。・医療機関等の定める規程等との内容と齟齬がある場合、サービス水準の問題になるので、合意を要する旨を追記した。 医療機関等との合意形成との関連：4.2.1(2)①参照
		(e) 機器を用いる場合は機器の管理	・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２ 【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．２．１．２【基本】） ・自社で定める機器の管理等の運用管理の規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(4)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）			ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
		（f）個人情報の記録媒体の管理（保管・授受等）の方法	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・自社で定める個人情報を記録した媒体の運用管理規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000 件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱うこと。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 ・個人情報の取扱につき、医療情報の重要性に伴う措置を含めた。。 医療機関等との合意形成との関連：4.2.1(2)②、(4)参照
		（g）患者等への説明と同意を得る方法	・医療機関等の管理者が患者等への説明及び同意を得る際に、事業者が提供する情報の範囲、事業者の役割等について医療機関等と合意すること。	追記理由： ・医療機関等の管理者が患者等への説明及び同意を得る際の情報提供の範囲、役割等を合意するため。 医療機関等との合意形成との関連：4.2.1(7)参照
		（h）監査	・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること （Ⅱ．３．１．２【基本】） ・ASP・SaaS サービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。（Ⅱ．４．３．２【基本】） ・自社において実施するシステム監査等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・監査記録等を医療機関等に開示する情報の範囲・条件等について合意すること。	追記理由： ・監査記録等は、セキュリティ上、ASP・SaaS 事業者の秘密にあたるものも含まれるので、開示の範囲、条件等を定めるため。 医療機関等との合意形成との関連：4.2.1(3)①、(5)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）			ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
		（i）苦情・質問の受け付け窓口	・ASP・SaaS サービスの提供に支障が生じた場合には、その原因が連携 ASP・SaaS 事業者に起因するものであったとしても、利用者と直接契約を結ぶ ASP・SaaS 事業者が、その責任において一元的にユーザサポートを実施すること。（Ⅱ．８．１．１【基本】） ・医療機関等の管理者側からの問合せ窓口を設けること。また受付の時間帯等について、医療機関等と合意すること。	追記理由： ・医療機関等の管理者からの問い合わせ体制を明記する旨を追記した。また問合せの対応時間等をサービス内容として合意するため。 医療機関等との合意形成との関連：4.2.1(3)③、(5)参照

３．２．２　物理的安全管理策

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、物理的安全管理対策について、第 6 章 6.4 に記述している。

（２） ASP・SaaS事業者への要求事項

物理的安全管理対策における ASP・SaaS 事業者への要求事項について表３-２に整理する。

表 3-2　物理的安全管理対策における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。	・サーバルームやラックの鍵管理を行うこと。（Ⅲ．４．４．６【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・バックアップ媒体も含め、個人情報を含むサーバ以外の機器・媒体等の保管場所を施錠管理すること。	追記理由： ・個人情報を含むサーバ以外の機器、媒体等の保管場所も施錠管理するため。
最低限	2.　個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。 　ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３　【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．４．４．１【基本】） ・重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。（Ⅲ．４．４．２【推奨】） ・委託業務に基づき受託する個人情報の内容を参照する必要が生じる場合には、データアクセスが可能な端末が設置されている部屋に対する入退出の施錠管理及び入退出管理を行うこと。	追記理由： ・個人情報に関するデータアクセスが可能な端末が設置されている部屋の施錠管理及び入退出管理につき、追記した。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	3.　個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．４．４．１【基本】）	
最低限	4.　個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。	・サーバルームやラックの鍵管理を行うこと。（Ⅲ．４．４．６【基本】） ・受託する個人情報を保守に用いる端末に保存しない旨、自社の運用管理規程等に定めること。	追記理由： ・保守用端末に受託した個人情報の保管を禁じるため。
最低限	5.　窃視防止の対策を実施すること。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３ 【基本】）	
推奨	1. 防犯カメラ、自動侵入監視装置等を設置すること。	・重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。（Ⅲ．４．４．２【推奨】）	

３．２．３　技術的安全管理策

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、技術的安全管理対策について、第 6 章 6.5 に記述している。

（２） ASP・SaaS事業者への要求事項

技術的安全管理対策における ASP・SaaS 事業者への要求事項について表３-３に整理する。

表 3-3　技術的安全管理対策における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　情報システムへのアクセスにおける利用者の識別と認証を行うこと	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	
最低限	2.　本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。	・同上	
最低限	3.　入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること。	・受託情報を扱う運用端末に、クリアスクリーン等の防止策を講じることを、自社の運用管理規程等に定めること。	追記理由： ・受託情報を扱う運用端末におけるクリアスクリーン等の防止策を講じるため。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	4.　動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	・データベースに格納されたデータの暗号化を行うこと。（Ⅲ．２．２．２【推奨】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・受託した情報の処理に必要な、システムに関する動作確認に際し、原則個人情報を含むデータを使用せず、テスト用のデータを使用すること。 ・システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること。	追記理由： ・情報セキュリティガイドラインでは動作確認については含まれていないため、動作確認で使用するデータ及び、個人情報を含むデータを使用する際の条件について追記した。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	5.　医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・提供するサービスにおいて、医療機関等の利用者の職種、担当業務等に応じたアクセス制御が可能な機能を含めること。 ・医療機関等の利用者の職種等に応じたアクセス制御の設定に関しては、医療機関等の管理者と協議の上、実際に設定する作業に関する役割も含めて合意すること。 ・医療機関等のアクセス管理に関する運用管理規程の内容に従った運用を行い、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・医療機関等の利用者の職種、担当業務等の設定に応じたアクセス制御をサービス仕様に含める旨を追記した。 ・医療機関等の定める規程等との内容との整合性をとることについて追記した。 医療機関等との合意形成との関連：4.2.1(5)、4.2.2(1)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	6.　アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。 情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。（Ⅲ．１．１．５【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】※ベストプラクティス(i)を実施すること。）	
最低限	7.　アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２　【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・運用管理者とログのレビュー者のアクセス権を分離する等の、アクセスログの改ざん等に対する措置を講じること。	追記理由： ・運用管理者等によるアクセスログの不当な削除、改ざん、追加等の防止策について追記した。
最低限	8.　アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。（Ⅲ．１．１．５【基本】※ベストプラクティスの(i)～(iv)を実施すること）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	9.　システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと。	・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．１．１．６【基本】） ・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。（Ⅲ．２．２．１【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	10. パスワードを利用者識別に使用する場合システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい)され、適切な手法で管理及び運用が行われること。(利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること) (2) 利用者がパスワードを忘れたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。) また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し(最長でも 2 ヶ月以内)、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと。	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・自社において定めたパスワードポリシーが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・利用者のパスワード発行等に関する手続及び業務範囲について、医療機関等と合意すること。	追記理由： ・提供するサービスにおけるパスワードポリシーと医療機関等の定める規程等との内容との整合性をとるため。 ・パスワード発行等の手続及び業務範囲の役割分担を定めるため。 医療機関等との合意形成との関連：4.2.2(1)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	12. 無線 LAN を利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。 (2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線 LAN の適用に関しては、総務省発行の「安心して無線 LAN を利用するために」を参考にすること。	・医療機関等がASP・SaaSの利用に際して無線LANを利用する場合に、医療機関等の無線LANが必要なセキュリティ対策について、事業者の役割、範囲等について合意すること。	追記事項： ・医療機関等が ASP・SaaS の利用に際して無線 LAN を利用する場合に、セキュリティ対策への事業者の役割を明らかにするため。 医療機関等との合意形成との関連：4.2.2(2)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．４．２．１ 【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・医療情報について、医療機関等が行う情報資産分類の区分に従い、アクセス制御を行うこと。	追記理由： ・医療情報の重要性に応じたアクセス制御を行うため。
推奨	2. 離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。	・最低限 3.と同様の対応を行う。	
推奨	3. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。	・データベースに格納されたデータの暗号化を行うこと。(Ⅲ．２．２．２【推奨】) ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】） ・不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPS の導入等）を講じること。(Ⅲ．３．１．５【推奨】)	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	4.　パスワードを利用者識別に使用する場合以下の基準を遵守すること。 (1)　パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。 (2)　パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・自社において定めたパスワードポリシーが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由。 ・提供するサービスにおけるパスワードポリシーと医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.2(1)参照
推奨	5.　認証に用いられる手段としては、ID＋バイオメトリックスあるいは IC カード等のセキュリティ・デバイス＋パスワードまたはバイオメトリックスのように利用者しか持ち得ない 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・採用する認証手段・方式について、医療機関等と合意すること。	追記理由： ・採用する認証手段・方式について、医療機関等と合意するため。 医療機関等との合意形成との関連：4.2.2(1)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	6.　無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。	・医療機関等がASP・SaaSの利用に際して無線LANを利用する場合に、医療機関等の無線LANが必要なセキュリティ対策についての、事業者の役割、範囲等について合意すること。	追記理由： ・医療機関等が ASP・SaaS の利用に際して無線 LAN を利用する場合に、セキュリティ対策への事業者の役割を明らかにするため。 医療機関等との合意形成との関連：4.2.2(2)参照

３．２．４　人的安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、人的安全管理対策について、第 6 章 6.6 に記述している。

（２） ASP・SaaS事業者への要求事項

人的安全管理対策における ASP・SaaS 事業者への要求事項について表３-４に整理する。

表 3-4　人的安全管理対策における ASP・SaaS 事業者への要求事項

(1)　従業者に対する人的安全管理措置

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1．医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること		
	① 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．２ 【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．５．１．１ 【基本】）	
	② 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．５．２．１ 【基本】）	
	③ 従業者の退職後の個人情報保護規程を定めること。	・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．５．３．１ 【基本】）	

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
推奨	1. サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３ 【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅲ．４．４．３【基本】）	

(2) 事務取扱委託業者の監督及び守秘義務契約

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1. 病院事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。		
	① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること。	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．２ 【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．５．１．１ 【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
	② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなうこと。	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２ 【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	
	③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３ 【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅲ．４．４．３【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
	④ 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。	・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．２．２．１ 【基本】） ・情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。（Ⅱ．２．２．２ 【基本】） ・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携 ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．３．１．１ 【基本】） ・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２ 【基本】） ・外部組織に対して再委託等を行う場合には、事前に医療機関等の管理者に対して説明を行い、契約において体制を明確にすること。 ・外部組織に対して、自社と同等の個人情報保護指針等について遵守させること。 ・外部組織においても表 3-9（外部と個人情報を含む医療情報を交換する場合の安全管理における**ASP・SaaS**事業者への要求事項）について遵守させること。	追記理由： ・外部組織に再委託を行う場合の、医療機関等の管理者への説明、及び体制の明確化について追記した。 ・外部組織に対して、自社と同等の個人情報への対応を求めるため。 医療機関等との合意形成との関連：4.2.1(2)①、②、(3)①参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	2. プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．２ 【基本】） ・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．２．２．１ 【基本】） ・情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。（Ⅱ．２．２．２ 【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．５．１．１ 【基本】）	

３．２．５　情報の破棄

（１） 情報の破棄

厚生省ガイドラインでは、情報の破棄については、第 6 章 6.7 に記述している。

（２） ASP・SaaS事業者への要求事項

情報の破棄における ASP･SaaS 事業者への要求事項についてに表 ３-５に整理する。

表 3-5　情報の破棄における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．４．２．１ 【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．５．３．２【基本】） ・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(4)参照
最低限	2.　情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。	・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．５．３．２【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	3.　外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策　(2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。	・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．５．３．２【基本】） ・情報の破棄を実施した場合に、その内容を医療機関等に対して報告し、破棄記録等を提出すること。	追記理由： ・情報破棄に関する医療機関等に対する報告のため。
最低限	4.　運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．５．３．２【基本】） ・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(4)参照

３．２．６　情報システムの改造と保守

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、情報システムの改造と保守について、第 6 章 6.8 に記述している。

（２） ASP・SaaS事業者への要求事項

情報システムの改造と保守における ASP・SaaS 事業者への要求事項についてに表 3-6 に整理する。

表 3-6　情報システムの改造と保守における ASP・SaaS 事業者がとるべき対

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めること。	・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携 ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．３．１．１ 【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．５．１．１ 【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．５．３．２【基本】） ・受託した情報の処理に必要な、システムの動作確認に際し、原則個人情報を含むデータを使用せず、テスト用のデータを使用すること。 ・システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること。	追記理由： ・情報セキュリティガイドラインでは動作確認については含まれていないため、動作確認で使用するデータ及び、個人情報を含むデータを使用する際の条件について追記した。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	2.　メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２ 【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	3. そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。	・ネットワーク構成図を作成すること(ネットワークをアウトソーシングする場合を除く)。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。(Ⅲ. 3. 1. 1【基本】) ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。(Ⅲ. 3. 1. 2【基本】) ・利用者及び管理者(情報システム管理者、ネットワーク管理者等)等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。(Ⅲ. 3. 1. 3【基本】) ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。(Ⅲ. 3. 2. 1【基本】)	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	4.　保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．２．２．１ 【基本】） ・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．５．３．１ 【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等について合意すること。	追記理由： ・保守業務体制の変更が生じた際の、報告の範囲、内容等を明確にするため。 医療機関等との合意形成との関連：4.2.1(5)参照
最低限	5.　保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。	・サービス提供に必要な保守業務を行うに際して、医療機関等の管理者に対して書面等により作業の事前及び事後に通知を行うこと、及び事前の了解を必要とする作業等について医療機関等と合意すること。	追記理由： ・保守業務実施の際の、医療機関等の管理者からの事前及び事後の承認に関して補足した。 医療機関等との合意形成との関連：4.2.1(5)参照
最低限	6.　保守会社と守秘義務契約を締結し、これを遵守させること。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・サービス提供に際して、医療機関等と守秘義務契約を締結すること。	追記理由： ・医療機関等との守秘義務締結について追記した。 医療機関等との合意形成との関連：4.2.1(2)③参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	7.　保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(4)参照
最低限	8.　リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集すると共に、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２ 【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・サービス提供に必要なシステムの保守をリモートメンテナンスで行う場合の医療機関等の管理者に対する報告、承認等について、医療機関等と合意すること。	追記理由： ・リモートメンテナンスで保守を行う場合の医療機関等の管理者に対する報告等について追記した。 医療機関等との合意形成との関連：4.2.1(5)参照
最低限	9.　再委託が行われる場合は再委託する事業者にも保守会社と同等の義務を課すこと。	・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．２．２．１ 【基本】） ・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携 ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．３．１．１ 【基本】） ・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２ 【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	1. 詳細なオペレーション記録を保守操作ログとして記録すること。	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２ 【基本】）	
推奨	2. 保守作業時には病院関係者立会いのもとで行うこと。	・サービス提供に必要な保守業務を医療機関施設内で行う際に、医療機関等の立会いの下で実施する旨を、医療機関等と合意すること。	追記理由： ・保守業務実施の際の、医療機関等の立会いに関して追記した。 医療機関等との合意形成との関連：4.2.1(5)参照
推奨	3. 作業員各人と保守会社との守秘義務契約を求めること。	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．２ 【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】）	
推奨	4. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２ 【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、医療機関等の管理者による監査の内容、範囲について、医療機関等と合意すること。	追記理由： ・社外への個人情報の持ち出しに関する記録及び報告について追記した。 医療機関等との合意形成との関連：4.2.1(5)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	5.　保守作業にかかわるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	

３．２．７　情報および情報機器の持ち出しについて

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、３．１．７情報および情報機器の持ち出しについて、第 6 章 6.9 に記述している。

（２） ASP・SaaS事業者への要求事項

情報および情報機器の持ち出しにおける ASP・SaaS 事業者への要求事項について表 3-7 に整理する。

表 3-7　情報および情報機器の持ち出しにおける ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(3)参照
最低限	2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(3)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	3. 情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・自社において定めた機器･媒体の盗難、紛失が生じた際の対応についての手順等が､医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ･医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(4)参照
最低限	4. 運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．５．２．１ 【基本】） ・従業員が、情報セキュリティポリシーもしくは ASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．５．２．２ 【基本】）	
最低限	5. 医療機関等や情報の管理者は、情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】）	
最低限	6. 情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】）	
最低限	8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。	・運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．５．２．１【基本】） ・受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・事業者において、受託情報を可搬媒体で持ち出し、処理を行わないとするため。
最低限	9. 持ち出した情報を、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わないこと。医療機関等が管理する情報機器の場合は、このようなソフトウェアをインストールしないこと。	・運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．５．２．１【基本】） ・受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・事業者において、受託情報を可搬媒体で持ち出し、処理を行わないとするため。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	10. 個人保有の情報機器（パソコン等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．５．２．１ 【基本】） ・従業員が、情報セキュリティポリシーもしくは ASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．５．２．２ 【基本】）	
推奨	1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３ 【基本】）	
推奨	2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	
推奨	3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】）	

３．２．８　災害等の非常時の対応

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、災害等の非常時の対応について、第 6 章 6.10 に記述している。

（２） ASP・SaaS事業者への要求事項

災害等の非常時の対応における ASP・SaaS 事業者への要求事項について表 3-8 に整理する。

表 3-8　災害等の非常時の対応における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1. 医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．４．２．１ 【基本】） ・自社において定めた非常時における BCP に関する運用手順等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連：4.2.1(4)参照
最低限	2. 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。		
最低限	3. 非常時の情報システムの運用 ・「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 ・非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監査をすること。 ・非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。	・自社において定めた非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・医療機関等の定める規程等との内容との整合性をとるため。 医療機関等との合意形成との関連 4.2.1(4)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、所管官庁への連絡を行うこと。	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。稼働停止を検知した場合は、利用者に速報を通知すること。（Ⅲ．１．１．１ 【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。障害を検知した場合は、利用者に速報を通知すること。（Ⅲ．１．１．２ 【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。また、利用者との取決めに基づいて、監視結果を利用者に通知すること。（Ⅲ．１．１．３ 【推奨】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。（Ⅲ．１．１．８【基本】） ・外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。（Ⅲ．３．２．５【推奨】） ・所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。	追記理由： ・所管官庁に対して法令に基づく資料提出のため、機器等の設置場所を制限するため。

３．２．９　外部と個人情報を含む医療情報を交換する場合の安全管理

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、外部と個人情報を含む医療情報を交換する場合の安全管理について、第 6 章 6.11 に記述している。

（２） ASP・SaaS事業者への要求事項

外部と個人情報を含む医療情報を交換する場合の安全管理における ASP・SaaS 事業者への要求事項について表 ３-９に整理する。

表 3-9　外部と個人情報を含む医療情報を交換する場合の安全管理における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1. ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策をとること。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】） ・不正な通過パケットを自動的に発見、もしくは遮断する措置（ID/IPS の導入等）を講じること。（Ⅲ．３．１．５【推奨】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．３．２．１【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】） ・医療機関等がASP・SaaSを利用するネットワークにつき、ウイルスや不正なメッセージの混入等による改ざんに対する防止措置についての事業者の役割の範囲について医療機関等と合意すること。	追記理由： ・医療機関等のネットワークで、ASP・SaaS を利用するものの安全性を確認し、必要な措置に対する責任分界を明らかにするため。 医療機関等との合意形成との関連：4.2.2(3)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	2.　データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】） ・ASP・SaaSを利用するネットワークで用いられる医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、医療機関等から事業者までの確認を行うこと（但し事業者が保守業務を再委託している場合には、事業者と再委託先との接続では本項の対応を適用せず、別途なりすましを防止する策を講じること）。 ・厚生労働省ガイドラインに基づいて医療機関等が採用する通信方式認証手段が妥当なものであることを確認することにつき、事業者の役割と範囲を、医療機関等と合意すること。	追記理由： ・医療機関等が ASP・SaaS を利用するネットワークに用いる機器におけるアクセス制御の状況を確認し、必要な措置を講じる際の事業者の責任分界を明らかにするため。 医療機関等との合意形成との関連：4.2.2(3)参照
最低限	3.　施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策をとること。これに関しては、医療情報の安全管理に関するガイドライン「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。	表 3-3 参照のこと	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	4.　ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。	・不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPS の導入等）を講じること。（Ⅲ．３．１．５【推奨】） ・ASP・SaaSを利用するネットワークで用いられるルータ等のネットワーク機器が厚生労働省ガイドラインで求める安全性が確認されているものであること、ASP・SaaSを利用するネットワークで用いられる医療機関等の施設内のルータについて、これを経由して医療機関等の施設間を結ぶVPNの間で送受信ができないように経路設定されていること等に関して、事業者の役割、範囲を医療機関等と合意すること。	追記理由： ・医療機関等がASP・SaaSを利用するネットワークで用いられるルータ等のネットワーク機器の安全性、必要な設定が施の確認等についての事業者の責任分界を明らかにするため。 医療機関等との合意形成との関連：4.2.2(3)参照
最低限	5.　送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・ASP・SaaSにおいて送受信されるデータに対して、電子政府推奨の暗号鍵を用いた暗号化等によるセキュリティ対策を講じること。 ・暗号化によるセキュリティ対策が、医療機関等が求める水準を満たすものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	追記理由： ・ASP・SaaS において送受信されるデータに対する暗号化等によるセキュリティ対策について補足した。 医療機関等との合意形成との関連：4.2.2(3)参照

	医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）	ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	6. 医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。 そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通または著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処 また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。 ・患者等に対する説明責任の明確化。 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。 ・交換した医療情報等に対する管理責任及び事後責任の明確化。 ・ 個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２ 【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・通常運用時、緊急時の医療機関等と事業者との起点から終点までの通信手順を明確にし、事業者の負う責任の範囲、役割等について、医療機関等と合意すること。 ・医療機関等の管理者において発生する患者等に対する説明責任、管理責任等、各種責任に関し、事業者が負う責任の範囲、役割等について、医療機関等と合意すること。	追記理由： ・事業者と医療機関等間の通信における責任分界を明確にするため。 ・ASP・SaaS を利用する医療機関等が発生する責任の内部分担についての、責任分 界、範囲、役割分担等を明確にするため。 医療機関等との合意形成との関連：4.2.1(6)参照

	医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）	ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	7. リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】）	
最低限	8. 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また上記 1 及び 4 を満たしていることを確認すること。	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ．２．１．４【推奨】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・<u>サービスを提供する際に用いる回線の管理責任、品質等に対する事業者の責任の範囲、役割等について、医療機関等と合意すること。</u>	追記理由： ・ASP・SaaS 提供契約を行う際の、サービスを提供する際に用いる回線に対する管理責任の範囲、品質等に対する責任分界を明確にするため。 医療機関等との合意形成との関連：4.2.1(6) 、4.2.2(3)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	9.　患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信の SSL 暗号化、PKI 個人認証等の技術を用いた対策を実施すること。 　また、情報の主体者となる患者等へ危険性や提供目的の納得できる説明を実施し、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】） ・患者が情報を閲覧する情報システムの安全性に関する説明責任等において、事業者は責任の範囲、役割等について、医療機関等と合意すること。	追記理由： ・患者が情報を閲覧する情報システムの安全性に関する説明責任等の責任分界を明らかにするため。 医療機関等との合意形成との関連：4.2.2(3)参照
推奨	1.　やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いると共に運用等の要件を設定すること。	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・医療機関等の利用者が、医療機関の外部からASP・SaaSを利用する場合に、事業者は、医療機関の利用者が用いるPCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップ等の技術導入に関する事業者の役割、範囲等を医療機関等と合意すること。	追記理由： ・医療機関等の利用者が利用するための仮想デスクトップ等の技術導入における事業者の役割、範囲等を明らかにするため。 医療機関等との合意形成との関連：4.2.2(3)参照

３．２．１０　法令で定められた記名・押印を電子署名で行うことについて

（１） 厚生労働省ガイドラインの記述

厚生省ガイドラインでは、法令で定められた記名・押印を電子署名で行うことについて、第 6 章 6.12 に記述している。

（２） ASP・SaaS事業者への要求事項

法令で定められた記名・押印を電子署名で行うことに関する ASP・SaaS 事業者への要求事項について表 ３-１０に整理する。

表 3-１０　１法令で定められた記名・押印を電子署名で行うことに関する ASP・SaaS 事業者への要求事項

(1)　厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　保健医療福祉分野 PKI 認証局については、電子証明書内に医師等の保健医療福祉に係る資格が格納された認証基盤として構築されたものである。保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、この保健医療福祉分野 PKI 認証局の発行する電子署名を活用するのが望ましい。 ただし、当該電子署名を検証しなければならない者すべてが、国家資格を含めた電子署名の検証が正しくできることが必要である。	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子証明書、もしくは電子署名法の規定に基づく**認定特定認証事業者の発行する電子証明書**によるものであることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・法令で定められた記名・押印の電子署名の実施について、追記したため。 医療機関等との合意形成との関連：4.2.2(4)参照
最低限	2.　電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもＡの要件[4]を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。		
最低限	3.「電子署名に係る地方公共団体の認証業務に関する法律」（平成 14 年法律第 153 号）に基づき、平成 16 年 1 月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。		

[4]ここでは「電子署名及び認証業務に関する法律」 第２ 条１項の要件を指す。

(2)　電子署名を含む文書全体にタイムスタンプを付与すること。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1. タイ ムスタンプは、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの 安全な長期保存のために－」（総務省、平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能である事。	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子署名もしくはこれと同等の仕様を含むものであることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・法令で定められた記名・押印の電子署名の実施について、追記したため。 医療機関等との合意形成との関連：4.2.2(4)参照
最低限	2.　法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。		
最低限	3. タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。		

(3)　上記タイムスタンプを付与する時点で有効な電子証明書を用いること。

	医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）	ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1. 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値と共にその全体に対してタイムスタンプを付与する等の対策が必要である。	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子署名もしくはこれと同等の仕様を含むものであることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・法令で定められた記名・押印の電子署名の実施について、追記したため。 医療機関等との合意形成との関連：4.2.2(4)参照

３．３ 外部保存におけるASP・SaaS事業者への要求事項

医療情報の外部保存を行うための指針等を厚生労働省ガイドラインでは、「8 診療録及び診療諸記録を外部に保存する際の基準」に示しており、ASP・SaaS により外部保存する際の ASP・SaaS 事業者への要求事項もこれを満たすことが求められる。

また ASP・SaaS による外部保存は、電子保存が不可欠であり、この場合には厚生労働省ガイドライン「7 電子保存の要求事項について」に示される真正性、見読性、保存性を満たすことが求められる（8.1.1 電子保存の 3 基準の遵守)。

従って医療情報を ASP・SaaS により外部保存を行う際に事業者に求められる要求事項は、上記を満たす内容であることが必要である。

以下この整理を踏まえて、ASP・SaaS 事業者が医療情報の処理に際して行う外部保存において、求められる要求事項について記述する。

３．３．１ 外部保存に対する要求事項が求められる文書

外部保存の要求事項が求められる文書は、厚生労働省ガイドラインの 3.2 に示されて通り、外部保存改正通知で定められた表 3-1 1に示す文書が対象となる。

また、表 3-1 1に示す文書等がその法定保存年限を経過する等の事由によって、施行通知[5]や外部保存改正通知の対象外となった場合にも、外部保存を実施（継続）する場合には、３．３．２～３．３．５に準じて取扱うことが求められる(厚生労働省ガイドライン 3.3)。

[5]本ガイドラインで「施行通知」とは、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 17 年 3 月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号 厚生労働省医政局長・医薬食品局長・保険局長連名通知）をいう。

表 3-１１　外部保存が可能な文書等（厚生労働省ガイドライン 3.2 より作成）

文書等
医師法(昭和 23 年法律第 201 号)第 24 条の診療録
歯科医師法(昭和 23 年法律第 202 号)第 23 条の診療録
保健師助産師看護師法(昭和 23 年法律第 203 号)第 42 条の助産録
医療法（昭和 23 年法律第 205 号）第 51 条の 2 第 1 項及び第 2 項の規定による事業報告書等及び監事の監査報告書の備置き
医療法(昭和 23 年法律第 205 号)第 21 条、第 22 条及び第 22 条の 2 に規定されている診療に関する諸記録及び同法第 22 条及び第 22 条の 2 に規定されている病院の管理及び運営に関する諸記録
歯科技工士法(昭和 30 年法律第 168 号)第 19 条の指示書
外国医師又は外国歯科医師が行う臨床修練に係る医師法第 17 条及び歯科医師法第 17 条の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条の診療録
救急救命士法(平成 3 年法律第 36 号)第 46 条の救急救命処置録
医療法施行規則（昭和 23 年厚生省令第 50 号）第 30 条の 23 第 1 項及び第 2 項の帳簿
保険医療機関及び保険医療養担当規則(昭和 32 年厚生省令第 15 号)第 9 条の診療録等（作成については、同規則第 22 条）
臨床検査技師等に関する法律施行規則（昭和 33 年厚生省令第 24 号）第 12 条の 3 の書類（作成については、同規則第 12 条第 14 号及び第 15 号）
歯科衛生士法施行規則(平成元年厚生省令第 46 号)第 18 条の歯科衛生士の業務記録
診療放射線技師法（昭和 26 年法律第 226 号）第 28 条第 1 項の規定による照射録

３．３．２　真正性の確保におけるASP・SaaS事業者への要求事項

真正性の確保に関する要求事項については、厚生労働省ガイドラインでは、7.1 に記述される。これを踏まえた ASP・SaaS 事業者への要求事項を表 3-１２に整理する。ASP・SaaS 事業者において外部保存する場合には、基本的事項（厚生労働省ガイドラインでは「医療機関等に保存する場合」に記述）に記述する事項に加えて、医療機関等以外に保存する際の要求事項（厚生労働省ガイドラインでは「ネットワークを通じて医療機関等の外部に保存する場合」に記述）に記述する事項についても参照されたい。

表 3-12　真正性の確保における ASP・SaaS 事業者への要求事項

基本的事項（厚生労働省ガイドラインでは【医療機関等に保存する場合】に記述）

（1）　作成者の識別及び認証

a. 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　利用者を正しく識別し、認証を行うこと。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	
最低限	2.　システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある利用者以外による作成、追記、変更を防止すること。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・提供する電子カルテシステム等に関するサービスにおいて、医療機関等の職務権限等に応じたアクセス制御が可能であることを含め、仕様内容について、医療機関等と合意すること。	追記理由：・医療機関等の職務権限等に応じたアクセス制御に対応すべき旨を補足した。 医療機関等との合意形成との関連：4.2.3(1)参照

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	3.　業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。	・同上	・同上

b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置もしくはシステムにより記録が作成される場合

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1.　装置の管理責任者や操作者が運用管理規程で明確にされ、管理責任者、操作者以外による機器の操作が運用上防止されていること。	・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	追記理由： ・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースに関する事業者の役割、範囲等を明らかにするため。 医療機関等との合意形成との関連：4.2.3(1)参照
最低限	2.　当該装置による記録は、いつ・誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。	・同上	・同上

(2) 記録の確定手順の確立と、作成責任者の識別情報の記録

a. 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1. 診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時が含まれること。	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。(Ⅲ．１．１．５【基本】) ・電子データの原本性確保を行うこと。(Ⅲ．５．１．１【推奨】)	
最低限	2. 「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。	・入力された内容が記録の確定前に作成責任者によって確認できる仕様とすることを、医療機関等と合意すること。	追記理由： ・入力された内容が記録の確定前に作成責任者によって確認できる仕様とすることに対応するため。 医療機関等との合意形成との関連：4.2.3(1)参照
最低限	3. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。(Ⅱ．２．１．３ 【基本】) ・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。(Ⅱ．３．１．２ 【基本】) ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。(Ⅲ．２．１．３【基本】) ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。(Ⅲ．２．３．１【基本】)	

b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置もしくはシステムにより記録が作成される場合

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　運用管理規程等に当該装置により作成された記録の確定ルールが定義されていること。その際、作成責任者の氏名等の識別情報（または装置の識別情報）、信頼できる時刻源を用いた作成日時が記録に含まれること。	・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	追記理由： ・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースに関する事業者の役割、範囲等を明らかにするため。 医療機関等との合意形成との関連：4.2.3(1)参照
最低限	2.　確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	・同上	・同上

(3)　更新履歴の保存

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1.　一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せることができること。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２ 【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せられる機能を含めること。 ・更新管理の仕様について、医療機関等と合意すること。	追記理由： ・データ保存における更新管理に関する仕様を明らかにするため。 医療機関等との合意形成との関連：4.2.3(1)参照
最低限	2.　同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。	・同上	・同上

(4) 代行操作の承認機能

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1. 代行操作を運用上認めるケースがあれば、具体的にどの業務等に適用するか、また誰が誰を代行してよいかを運用管理規程で定めること。	・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。(Ⅲ. ３. １. ２【基本】) ・代行操作を実施するIDや運用方法について、予め医療機関等の管理者と内容を合意すること。	追記理由： ・代行操作に関する手順等を明らかにするため。 医療機関等との合意形成との関連：4.2.3(1)参照
最低限	2. 代行操作が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行操作の都度記録されること。	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。(Ⅲ. ２. １. ３【基本】)	
最低限	3. 代行操作により記録された診療録等は、できるだけ速やかに作成責任者による「確定操作（承認）」が行われること。	・代行操作された際の、データの確定に関する仕様について、医療機関等の管理者と内容を合意すること。	追記理由： ・代行操作によるデータ確定の仕様について追記した。 医療機関等との合意形成との関連：4.2.3(1)参照
最低限	4. 一定時間後に記録が自動確定するような運用の場合は、作成責任者を特定する明確なルールを策定し運用管理規程に明記すること。	・同上	・同上

（5） 機器・ソフトウェアの品質管理

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1. システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。	取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・機器、ソフトウェア構成について、医療機関等と合意をとること。 ・機器、ソフトウェア構成について文書化を行い、医療機関等の管理者に対して報告できる内容とすること。	追記理由： ・ASP・SaaS に用いるシステム仕様の文書化について追記した。 医療機関等との合意形成との関連：4.2.1(5)、4.2.3(1)参照
最低限	2. 機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されていること。	・提供するサービスにおけるシステムの導入プロセスについて、文書化を行うこと。 ・システムの構成管理内容を示す資料の開示内容・範囲・条件について、医療機関等と合意すること。	追記理由： ・ASP・SaaS に用いるシステムの導入プロセスの文書化について追記した。 ・ASP・SaaS に用いるシステムの構成管理の報告について追記した。 医療機関等との合意形成との関連：4.2.1(5)参照
最低限	3. 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。	・運用・操作に関する利用者教育における事業者の役割、範囲等について、医療機関等と合意すること。	追記理由： ・利用者教育における役割、範囲等を明らかにするため。
最低限	4. システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。	・システム構成やソフトウェアの動作状況に関する内部監査について、事業者の役割、範囲等について医療機関等と合意すること。	追記理由： ・システム構成やソフトウェアの動作状況に関する内部監査における役割、範囲等を明らかにするため。

医療機関等以外に保存する際の要求事項（厚生労働省ガイドラインでは【ネットワークを通じて医療機関等の外部に保存する場合】に記述）

医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

（１） 通信の相手先が正当であることを認識するための相互認証をおこなうこと

医療機関等の管理者への要求事項（厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項（情報セキュリティ対策ガイドラインの記述と下線部は本ガイドラインで追記した記述）	付記事項
最低限	診療録等のオンライン外部保存を受託する機関と委託する医療機関等が、お互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】）	

（２） ネットワーク上で「改ざん」されていないことを保証すること

医療機関等の管理者への要求事項（厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項（情報セキュリティ対策ガイドラインの記述と下線部は本ガイドラインで追記した記述）	付記事項
最低限	ネットワークの転送途中で診療録等が改ざんされていないことを保証できること。なお、可逆的な情報の圧縮・回復ならびにセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにはあたらない。	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．３．２．１【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】）	

（3） リモートログイン機能を制限すること

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	保守目的等のどうしても必要な場合を除き行なえないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。 なお、これらの具体的要件については 「6.11 外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照すること。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・ASP・SaaS提供に必要なシステムの保守をリモートメンテナンスで行う場合の、医療機関等への報告対象とするシステムの範囲、そのシステムに対するリモートメンテナンスの実施条件、報告内容等について、医療機関等と合意すること。	追記理由： ・リモートメンテナンスで保守を行う場合の医療機関等の管理者に対する運用方法等について合意するため。 医療機関等との合意形成との関連：4.2.1(5)参照

３．３．３ 見読性の確保におけるASP・SaaS事業者への要求事項

見読性の確保に関する要求事項については、厚生労働省ガイドラインでは、7.2に記述される。これを踏まえて、ASP・SaaS事業者への要求事項を表 ３-１３に整理する。ASP・SaaS において、外部保存するデータが、医療機関等にある場合には、「保存する場所について共通する内容」及び「医療機関等に保存する場合」に記述する事項についてのみ参照する必要がある。電子保存するデータが ASP・SaaS 事業者にある場合には、上記に加えて、「ネットワークを通じて医療機関等の外部に保存する場合」に記述する事項についても参照する必要がある。

表 3-13　見読性の確保における ASP・SaaS 事業者への要求事項

【保存する場所について共通する内容】

（1）情報の所在管理

医療機関等の管理者への要求事項（厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項（情報セキュリティ対策ガイドラインの記述と下線部は本ガイドラインで追記した記述）	付記事項
最低限	紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者毎の情報の全ての所在が日常的に管理されていること。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】）	

（2）見読化手段の管理

医療機関等の管理者への要求事項（厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項（情報セキュリティ対策ガイドラインの記述と下線部は本ガイドラインで追記した記述）	付記事項
最低限	電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。	・見読性を保証するサービス仕様について、医療機関等と合意すること。	追記理由： ・見読性を保証するサービス仕様について合意するため。 医療機関等との合意形成との関連：4.2.3(2)参照

（3）見読目的に応じた応答時間

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	目的に応じて速やかに検索表示もしくは書面に表示できること。	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。稼働停止を検知した場合は、利用者に速報を通知すること。（Ⅲ．１．１．１ 【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。また、利用者との取決めに基づいて、監視結果を利用者に通知すること。（Ⅲ．１．１．３ 【推奨】） ・ASP・SaaS サービスを利用者に提供する時間帯を定め、この時間帯における ASP・SaaS サービスの稼働率を規定すること。また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。（Ⅲ．２．１．１【基本】） ・見読性を保証するサービス仕様について、医療機関等と合意すること。	追記理由： ・見読性を保証するサービス仕様について合意するため。 医療機関等との合意形成との関連：4.2.3(2)参照

（4）システム障害対策としての冗長性の確保

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化や代替え的な見読化手段を用意すること。	・障害等が生じた場合等を想定し、冗長性を確保する仕様等について医療機関等と合意すること。	追記理由： ・障害等が生じた場合を想定して、冗長性を確保する仕様等を明らかにするため。 医療機関等との合意形成との関連：4.2.3(2)参照

【ネットワークを通じて外部に保存する場合】

医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。

（1）緊急に必要になることが予測される診療録等の見読性の確保

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製または同等の内容を医療機関等の内部に保持すること。	・緊急時の医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等）をASP・SaaSにおいて含めることについて、医療機関等の管理者と協議し、合意すること。	追記理由 ・緊急時の医療機関等における診療録等の見読性の確保を支援する機能について明らかにするため。 医療機関等との合意形成との関連：4.2.3(2)参照

（2）緊急に必要になるとまではいえない診療録等の見読性の確保

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・障害等が生じた場合の責任分界を明確にし、稼動を保証するサービスの品質について医療機関等と合意すること。	追記理由 ・障害等が生じた場合の稼動を保証するサービスの品質等を明らかにするため。 医療機関等との合意形成との関連：4.2.3(2)参照

３．３．４ 保存性の確保におけるASP・SaaS事業者への要求事項

保存性の確保に関する要求事項については、厚生労働省ガイドラインでは、7.3に記述される。これを踏まえて、ASP・SaaS事業者への要求事項を表 ３-１４に整理する。ASP・SaaSにより外部保存を行う際、基本的事項（厚生労働省ガイドラインでは「医療機関等に保存する場合」に記述）に記述する事項に加えて、医療機関等以外に保存する際の要求事項（厚生労働省ガイドラインでは「ネットワークを通じて医療機関等の外部に保存する場合」に記述）に記述する事項についても参照されたい。

表 3-１４　保存性の確保における ASP・SaaS 事業者への要求事項

基本的事項（厚生労働省ガイドラインでは【医療機関等に保存する場合】に記述）

（1）　ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。	・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。（Ⅲ．２．２．１【基本】）	

（2）　不適切な保管・取扱いによる情報の滅失、破壊の防止

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．５．２．１ 【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	2.　システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１ 【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．４．２．１ 【基本】） ・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 　また、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。（Ⅲ．１．１．９【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】）	
最低限	3.　記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと。	・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 　また、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。（Ⅲ．１．１．９【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．４．４．１【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅲ．４．４．３【基本】）	
最低限	4.　電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	5.　各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。（Ⅲ．２．３．２【推奨】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・バックアップのき損箇所の確認に関する仕様、方法等ついて、医療機関等と合意すること。	追記理由： ・バックアップのき損箇所の確認に関する仕様、方法等を明らかにするため。 医療機関等との合意形成との関連：4.2.3(3)参照
推奨	1.　記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３　【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．４．４．１【基本】） ・サーバルームやラックの鍵管理を行うこと。（Ⅲ．４．４．６【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】）	
推奨	2.　サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．４．４．１【基本】） ・サーバルームやラックの鍵管理を行うこと。（Ⅲ．４．４．６【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	3.　診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。（Ⅲ．２．３．２【推奨】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・<u>バックアップされたデータに対して、内容が改ざんされていないことを確認できる仕様について、医療機関等と合意すること。</u>	追記理由 ・バックアップの改ざん確認ができる仕様を明らかにするため。 医療機関等との合意形成との関連：4.2.3(3)参照

(3)　記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1.　記録媒体が劣化する以前に情報を新たな記録媒体または記録機器に複写すること。記録する媒体及び機器毎に劣化が起こらずに正常に保存が行える期間を明確にし、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体または記録機器については、そのデータを新しい記録媒体または記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３ 【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】）	
推奨	1.　診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 もしくは RAID-6 相当以上のディスク障害に対する対策を取ること。	・<u>医療情報のデータを格納するサーバのディスクの障害対策について、医療機関等と合意する。</u>	・医療情報のデータを格納するサーバのディスクの障害対策の対応を明らかにするため。 医療機関等との合意形成との関連：4.2.3(3)参照

(4) 媒体・機器・ソフトウェアの整合性不備による復元不能の防止

医療機関等の管理者への要求事項 (厚生労働省ガイドラインの記述)		ASP・SaaS 事業者への要求事項 (情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述)	付記事項
最低限	1. システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。	・入出力するデータ項目の形式ついて、標準形式を採用する。標準形式によることができない場合には、妥当なデータ項目の形式について医療機関等と合意すること。	追記理由： ・入出力するデータ項目形式の採用につき、原則標準形式を採用し、これによることができない場合に医療機関等と合意するため。 医療機関等との合意形成との関連：4.2.3(3)参照
最低限	2. マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。	・マスターテーブルの変更に際してのレコード管理方法・とるべき措置等について、移行に際して情報内容の変更が生じない機能及び検証方法を備える。本機能を備えることが困難な場合には、妥当な提案を行い、医療機関等と合意すること。	追記理由： ・マスターテーブルの移行に際し、原則情報内容の変更が生じない機能及び検証方法を採用し、これによることができない場合、妥当な提案の上、医療機関等と合意するため。 医療機関等との合意形成との関連：4.2.3(3)参照

医療機関等以外に保存する際の要求事項（厚生労働省ガイドラインでは【ネットワークを通じて医療機関等の外部に保存する場合】に記述）
医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

（1）データ形式及び転送プロトコルのバージョン管理と継続性の確保をおこなうこと

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップまたは変更されることが考えられる。その場合、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。	・ASP・SaaSによりデータ保存する際に用いるデータ形式及び転送プロトコルを変更する場合、変更前の方式との互換性の確保等について、医療機関等と合意する。	追記理由： ・ASP・SaaS によりデータ保存する際に用いるデータ形式及び転送プロトコルを変更する場合、変更前の方式との互換性の確保等について追記した。 医療機関等との合意形成との関連：4.2.3(3)参照

（2）ネットワークや外部保存を受託する機関の設備の劣化対策をおこなうこと

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策をおこなうこと。	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。（Ⅲ．１．１．４【推奨】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．２．１．２【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ．２．１．４【推奨】） ・ASP・SaaSに用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意すること。	追記理由： ・ASP・SaaS に用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について追記した。 医療機関等との合意形成との関連：4.2.1(5)、4.2.3(3)参照

（1）ネットワークや外部保存を受託する機関の設備の互換性を確保すること

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って､外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し､安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。	ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．２．１．２【基本】） ・ASP・SaaSに用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意すること。	追記理由： ・ASP・SaaS に用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について追記した。 医療機関等との合意形成との関連：4.2.1(5) 、4.2.3(3)参照

３．３．５　外部保存におけるASP・SaaS事業者への要求事項

ここでは厚生労働省ガイドラインの「8.1.2 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準」及び「8.1.3 個人情報の保護」に基づいて、電子保存を行う場合に、ASP・SaaS 事業者の対応すべき内容について、記述する。

（１） 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準におけるASP・SaaS事業者への要求事項

厚生労働省ガイドラインでは、外部保存を受託する機関として、3 つのケースを想定している。

① 病院、診療所、医療法人等が適切に管理する場所に保存する場合
② 行政機関等が開設したデータセンター等に保存する場合
③ 医療機関等の委託を受けて情報保管する民間等のデータセンターに保存する場合

ASP・SaaS においては、③により外部保存を行うことが一般的であることから、以下では③に対応する ASP・SaaS 事業者への要求事項を表 3-15 に整理する。

表 3-１５　外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	（ア）医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。	・従業員が、情報セキュリティポリシーもしくは ASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．５．２．２　【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１　【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２　【基本】） ・守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わすこと。	追記理由： ・守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わすことを追記した。 医療機関等との合意形成との関連：4.2.1(2)③参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	（イ）医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．３．２．１【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。（Ⅲ．３．２．５【推奨】） ・ネットワーク回線を含めてASP・SaaS事業者がサービスを提供する場合、そのネットワークの安全性に関しては、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守すること。 ・自社で講じるネットワークの安全対策が、医療機関等が定めるネットワーク回線の安全性に関する基準を満たしていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・ネットワーク回線を含めてASP・SaaS 事業者がサービスを提供する場合、そのネットワークの安全性に関して、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守することを追記した。 ・医療機関等が定めるネットワーク回線の安全性に関する基準に合致したネットワークの安全対策を施すことを追記した。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	（ウ）受託事業者が民間事業者等に課せられたガイドライン等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２ 【基本】） ・ASP・SaaSにおける情報セキュリティ対策ガイドライン（平成 20 年 1 月 30 日総務省）及び本ガイドラインを遵守すること。 ・遵守すべきガイドラインの範囲及びこれを遵守している旨の報告につき、その内容・範囲等を、医療機関等と合意すること。	追記理由： ・ASP・SaaS における情報セキュリティ対策ガイドライン（平成 20 年 1 月 30 日総務省）及び本ガイドラインを遵守することを追記した。 ・遵守すべきガイドラインの範囲及びこれを遵守している旨の報告につき、その内容・範囲等につき、医療機関等等と合意する旨を追記した。 医療機関等との合意形成との関連：4.2.1(1)参照
最低限	（エ）保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３ 【基本】） ・受託した医療情報を、保守作業に必要な範囲での閲覧を超えて閲覧しないこと。 ・許可されていない受託データの閲覧を禁止することにつき、その方法等を含め、医療機関等と合意すること。	追記理由： ・受託した医療情報を、保守作業に必要な範囲での閲覧を超えて閲覧しないことを追記した。 ・許可されていない受託データの閲覧を禁止する範囲、方法等につき追記した。 医療機関等との合意形成との関連：4.2.3(2)参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	（オ）外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・受託した医療情報は、匿名化されたものを含めて、医療機関との契約に基づくことなく、分析、解析等を実施しないこと。 ・医療機関との契約に基づくことなく、受託したデータの分析・解析を実施しないことにつき、その方法等を含め、医療機関等と合意すること。	追記理由： ・受託データの分析・解析しないこと等を明らかにするため。 医療機関等との合意形成との関連：4.2.1(1)(エ)参照
最低限	（カ）保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等において情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	（キ）医療機関等において外部保存を受託する事業者の選定基準を定めること。少なくとも以下の４点について確認すること。 (a)　医療情報等の安全管理に係る基本方針・取扱規程等の整備 (b)　医療情報等の安全管理に係る実施体制の整備 (c)　実績等に基づく個人データ安全管理に関する信用度 (d)　財務諸表等に基づく経営の健全性	・契約に先立ち、医療機関等の管理者から、選定に必要な情報の提供を求められた場合に、速やかに提出すること。	追記理由： ・事業者選定のための資料の提供を可能な範囲で行うため。
推奨	（ウ）「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等の委託を受けて情報を保管する民間等のデータセンターに保存する場合」では、技術的な方法としては、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
推奨	（エ）外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「(a)暗号化を行う」、「(b)情報を分散管理する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・<u>システム管理者のデータアクセスの制限の方法について、医療機関等と合意する。</u>	追記理由： ・医療機関等の利用者以外に、システム管理者においてもデータアクセスの制限の方法について明らかにするため。 医療機関等との合意形成との関連：4.2.3(2)参照

（２） 個人情報の保護におけるASP・SaaS事業者への要求事項

個人情報保護について、厚生労働省ガイドラインでは、8.1.3 に記述されている。これを踏まえて、ASP・SaaS 事業者への要求事項を表 3-１６に整理する。

表 3-１６　個人情報保護における ASP・SaaS 事業者への要求事項

（１）　診療録等の外部保存委託先の事業者内における個人情報保護

	医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）	ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	① 適切な委託先の監督を行なうこと 診療録等の外部保存を受託する事業者内の個人情報保護については「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」において考え方が示されている。「Ⅲ 医療・介護関係事業者の義務等」の「4. 安全管理措置、従業者の監督及び委託先の監督(法第 20 条～第 22 条)」及び本指針 6 章を参照し、適切な管理を行なうこと。	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。(Ⅱ．７．１．１ 【基本】) ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。(Ⅱ．７．１．２ 【基本】) ・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。(Ⅱ．７．１．３ 【基本】) ・個人情報は関連する法令に基づいて適切に取り扱うこと。(Ⅲ．５．１．２【基本】) ・自社で定める個人情報保護を記録した媒体の運用管理規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000 件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	追記理由： ・ 医療機関等の定める規程等との内容との整合性をとることについて追記した。 医療機関等との合意形成との関連：4.2.1(2)②、(4)参照

（２）外部保存実施に関する患者への説明

診療録等の外部保存を委託する施設は、あらかじめ患者に対して、必要に応じて患者の個人情報が特定の外部の施設に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	① 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始するべきである。	・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、医療機関等と合意すること。	追記理由： ・医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等を合意する旨につき追記した。 医療機関等との合意形成との関連：4.2.1(7)参照
	② 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明をし、理解を得ればよい。		追記理由： ・事業者の責任分界の範囲外であり、本ガイドラインの安全要求事項としては扱わない。

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）		ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
	③ 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。		追記理由： ・事業者の責任分界の範囲外であり、本ガイドラインの安全要求事項としては扱わない。

３．４ ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項

３．４．１　ASP・SaaS の提供終了が発生する場面

ASP・SaaS の提供終了が発生する場面については、以下の 2 つがある。

・ASP・SaaS 事業者の都合によりサービス提供を終了するケース

・医療機関等の都合により、サービス提供を終了するケース

いずれの場合にも、ASP・SaaS 事業者は受託データの破棄及びその報告を行う必要がある。またそれぞれの場面において、

・サービス提供契約終了の事前通知

・ASP・SaaS 事業者が受託するデータ等の引渡し

等を行うことが求められる。

３．４．２ ASP・SaaSの提供終了における実施項目

ASP・SaaS の提供終了に関し、厚生労働省ガイドラインでは、「8.4.2 外部保存契約終了時の処理について」において、外部保存終了時の考え方を記述している。この考え方に基づいて、ASP・SaaS の提供終了における ASP・SaaS 事業者の対応すべき内容を整理して表 3-１７に示す。

３．４．３　ASP・SaaS事業者間のサービス移行における留意点

ASP・SaaS 事業者においては、自社のサービス提供終了後、医療機関等が他の事業者に移行する際に、可能な限り円滑な移行進めるための協力を医療機関の求めに応じて行うことが求められる。

また ASP・SaaS において使用するデータの形式等についても、将来的な移行を視野に入れた対応をすることが望ましい。入出力するデータ項目の形式等について、標準形式を採用し、標準形式によることができない場合には、妥当な対応を行う旨を医療機関等と協議する、等の対応を図ることが求められる。

なお受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「5 情報の相互運用性と標準化について」に従って行うことが求められる。

表 3-１７　ASP・SaaS の提供終了における ASP・SaaS 事業者への要求事項

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）	ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
診療録等が機微な個人情報であるという観点から、外部保存を終了する場合には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはならない。 診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、終了しなければならない診療録等は速やかに処理を行い、処理が厳正に執り行われたかを監査する義務を果たさなくてはならない。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。 これらの廃棄に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要がある。また、実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化した規定を作成しておくべきである。 これらの厳正な取り扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になりうるためであり、そのことに十分に留意しなければならない。 ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければならない。また電子媒体の場合は、バックアップファイルにつ	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１ 【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．５．３．２【基本】） ・事業者の都合により医療機関等に対してASP・SaaSの提供を終了する場合の事前通知の方法、終了が認められる理由、及び終了に向けての対応について、医療機関等と合意すること。 ・情報の破棄の実施に際し、報告の内容・範囲・提出すべき資料等について、医療機関等と合意すること。 ・ASP・SaaSの提供を終了する場合に、受託しているデータ及びこれに関連する資料の内容、範囲、条件等について、医療機関等と合意すること。 ・受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「5 情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意すること。	追記理由： ・事業者の都合により医療機関等に対して ASP・SaaS の提供を終了する場合の、理由及び終了に伴う対応に関して追記した。 ・サービス提供契約終了に関する事前通告について、追記した。 ・医療機関等に対して ASP・SaaS の提供を終了する場合の情報の破棄、及びその報告について追記した。 ・医療機関等に対して ASP・SaaS の提供を終了する場合に、医療機関等に対して、受託するデータ及び関連する資料の提供について、追記した。 ・受託データの医療機関へ引き渡す際に、厚生労働省ガイドライン「5 情報の相互運用性と標準化について」に従うため。 医療機関等との合意形成との関連：4.2.1(5)、 (6)、(7)、(8)①、②参照

医療機関等の管理者への要求事項 （厚生労働省ガイドラインの記述）	ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
いても同様の配慮が必要である。 　また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想される。従って、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはならない。		

第４章　安全管理の実施における医療機関等との合意形成の考え方

第３章では、ASP・SaaS事業者が医療情報サービスを提供するにあたり、安全管理の観点から対応すべき内容についてまとめた。ASP・SaaS事業者にとって、情報セキュリティ対策ガイドラインの対策項目[6]は、サービス提供にあたって優先的に実施すべき内容であり、医療機関等からも基本的に「対策済み」であることが期待されている。これに対して、医療情報サービスの提供に特化して追記された内容については、医療機関等が求める責任分担やサービスレベルにかなり幅があるものが含まれており、提供コストも考慮しつつ、機関個別に最適な選択と合意形成を行う必要がある。具体的には、第３章で対応すべき内容として「医療機関等と合意すること」とされた項目がこれにあたる。

本章では、上で述べたような医療機関等が求める責任分担やサービスレベルにかなり幅がある安全管理上の対応内容に関し、ASP・SaaS 事業者と医療機関等が「何について合意しなければならないか」「形成された合意をどのようにして遵守するか」について記述する。

４．１ 契約、SLA等の合意文書の位置付け

医療機関等が ASP・SaaS を利用する場合、医療情報の取扱いを ASP・SaaS 事業者が受託することに伴い、医療機関等に課せられる責任を ASP・SaaS 事業者との間で分担する必要性が生じる。上で述べたように、この責任分担に各医療機関等の事情（提供コストに関することを含む）や利用している通信サービス等が大きく影響する場合には、ASP・SaaS 事業者と医療機関等が責任分界と役割分担について合意する必要がある。また、提供するサービスレベルが提供コストに大きく影響する安全管理上の対応については、業務要求とコストのバランスにおいて適切なサービスレベルを両者で合意することが求められる。

このような場合には、ASP・SaaS では契約書、SLA 等の文書において合意内容を明文化し、両当事者において遵守する必要がある。

なお、医療機関等と ASP・SaaS 事業者との合意内容については、情報セキュリティ対策ガイドライン及び本ガイドラインの内容を満たすものであることが求められる。

４．２ 安全管理の実施において医療機関等と合意形成を行なう内容

ここでは、第３章で「医療機関等と合意すること」と記された対応内容について、「何について合意しなければならないか」を中心にまとめる。これらは、以下の２種類に分類される。

[6] 正確には「基本」に分類される対策項目がこれにあたる。

1) 契約書等において定める対応内容
2) 契約期間中、あらかじめ規定した方法で客観的に計測し、定期報告等を行なう対応内容（サービスレベルに係る事項等）

1)は主として責任分担に関わることであり、2)は主として責任分担の状況を前提としたサービスレベル保証に関わることである。以下で「契約、SLA 等で明文化すること」が求められた場合、明文化の方法は、概ね 1)に該当する場合は契約書を中心に、2)に該当する場合は SLA を中心に記述するという考え方になる。

4.2.1 以降では、第 3 章の記述との参照関係を示している。明示するにあたっては、「表番号（最 or 推）項番」という標記形式を用いて、第 3 章における位置を示している。例えば 3-1(最)2 は、「第 3 章の表 3-1」の医療機関等の管理者への要求事項の「最低限」に書かれている、2.の項目に対応する実施項目であることを示す。同様に 3-1(推)1.は、表 3-1 の推奨するガイドラインの項番 1.に対応する記述項目であることを示す（図　4 - 1 参照）。

【関連する第3章の記述項目：3-1(最)1.】

「第3章の表3-1」の医療機関等の管理者への要求事項の「最低限」に書かれている、1.の項目に関連する項目であることを示す。

表 3-1　組織的安全管理対策におけるASP・SaaS事業者への要求事項

医療機関等の管理者への要求事項（厚生労働省ガイドラインの記述）		ASP・SaaS事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と 下線部は本ガイドラインで追記した記述）	付記事項
最低限	1.　情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【推奨】） ・各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。（Ⅱ．４．３．１【基本】） ・情報システム運用責任者を明確に定めて、合意すること。	追記理由： ・情報セキュリティガイドラインでは、情報資産の管理責任者について記述されているので、情報システム運用責任者として記述した。 ・管理責任者を医療機関等の管理者に対して明確にするため。 医療機関等との合意形成との関連：4.2.1(3)②参照

図　4 - 1　4.2.1 以降に示す第 3 章各表への参照を示す記述の見方

４．２．１　組織体制及び運用管理に係る対応内容

（１） 受託情報の取扱等

① 受託情報に関するリスク対応措置【関連する第 3 章の記述項目：3-4(最)(4)1.④、3-15(最)(d)】

ASP・SaaS 事業者は、医療機関等が定める医療情報に対するリスクアセスメントの内容、リスクの予防措置、事故への対応等に準じてリスク対応措置の内容を医療機関等と協議し、合意すること。特に医療機関等が実施する医療情報に対するリスクアセスメントの中で、受託する情報に対して ASP・SaaS 事業者が行うリスク対応と整合性がとれていることを確認すること。また両者が求めた場合には、合意した内容を契約、SLA 等に明文化すること。

なお、医療情報に対するリスクアセスメント等を医療機関等が定めていない場合には、ASP・SaaS 事業者が情報セキュリティ対策ガイドライン等に基づき定めているリスク対応措置に準じて対応することを、契約、SLA 等に明記すること。

② 受託した個人情報の取扱【関連する第 3 章の記述項目：3-1(最)4.、3-1(最)5.(f)、3-4(最)(2)1.④】

ASP・SaaS 事業者は、医療機関等が定める個人情報保護指針に準じて個人情報を取り扱うことを、契約、SLA 等で明記すること。

なお、医療機関等が個人情報保護指針を定めていない場合には、ASP・SaaS 事業者が定める個人情報保護指針等に準じて対応することを契約、SLA 等に明記すること。

この場合、ASP・SaaS 事業者が定めた個人情報保護指針等は、情報セキュリティ対策ガイドライン及び「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成１６年１２月２４日（平成１８年４月２１日改正）厚生労働省）の内容を満たすものであること。

③ 守秘義務契約【関連する第 3 章の記述項目：3-6(最)6、3-15(最)ア】

ASP・SaaS 事業者は受託する医療情報を対象範囲とする守秘義務契約を、医療機関等と締結すること。

④ 受託データの委託外解析の禁止【関連する第 3 章の記述項目：3-15(最)(エ)】

医療機関との契約に基づくことなく、受託したデータの分析・解析を実施しないことにつき、その方法等を含め、医療機関等と契約、SLA 等において明文化すること。

（２） 組織体制

① 医療機関等の体制に対応したASP・SaaS事業者の体制【関連する第３章の記述項目：3-1(最)5.(b)(h)、3-4(最)(2)1.④】

ASP・SaaS 事業者は、サービス提供の総括責任者を定めるとともに、サービス提供体制、文書管理体制、監査体制等について医療機関等と協議し、合意結果を契約、SLA 等において明文化すること。具体的には、以下の管理者等について明文化すること。

・システム管理者
・機器管理者
・運用責任者
・安全管理者
・個人情報保護責任者等
・監査責任者（内部監査、外部監査）

また、サービスを提供するにあたり、他社とのデータ連携、サービス連携、再委託等がある場合には、これらを含めた体制について契約、SLA 等に明文化すること。

② 情報システム運用管理者【関連する第３章の記述項目：3-1(最)1.】

ASP・SaaS 事業者は、①の体制の中で、ASP・SaaS 提供における情報システム運用管理者を契約、SLA 等に明記すること。

③ 医療機関等からの問合せに対する運用体制【関連する第３章の記述項目：3-1(最)5.(i)】

ASP・SaaS 事業者は、医療機関等からの問合せに対して、以下の内容につき医療機関等と協議し、合意すること。また、両者が求めた場合には、契約、SLA 等で明文化すること。

・医療機関等の管理者のための問合せ窓口等の運用体制、受付時間帯等
・患者等、医療機関等の管理者以外からの苦情、質問の受付を受託する場合の業務範囲及び受付時間帯等
・医療機関等の管理者が患者等への説明責任を果たす際に、ASP・SaaS 事業者が助力として行なう情報提供の範囲、情報の開示条件、事業者自身が説明を行う範囲等

（３） 規定類等に関する運用関連実施事項【関連する第３章の記述項目：3-1(最)2－5.、3-5(最)1.、4.、3-6(最)7、3-7(最)3、3-8(最)1.－2.】

ASP・SaaS 事業者は、医療機関等が定める情報システムの運用管理規程類等に準じてサービスを運用することを医療機関等と合意すること。特に医療機関等が策定する医療情報に関する運用管理規程の中で、受託する情報に関

対して ASP・SaaS 事業者が定める運用管理規程と整合性がとれていることを確認すること。また、両者が求めた場合には、合意された運用管理の内容やサービスレベルを契約、SLA 等で明文化すること。

一方、医療機関等が、情報システムの運用管理規程類等を定めていない場合には、ASP・SaaS 事業者が定めている同様の規程類に準じて対応することを契約、SLA 等に明記すること。但し、ASP・SaaS 事業者が定める運用管理規程類等は、情報セキュリティ対策ガイドライン及び本ガイドラインの内容を満たすものであること。

なお、ここで対象とする情報システムに関する運用管理規程類等とは以下のものである。

【運用管理規程類】
・個人情報保護規程
・運用管理規程（情報の持ち出しに関する手続を含むもの）
・アクセス管理規程（非常時のアカウント運用ルールを含むもの）
・機器管理等の規程
・データセンター及び受託した個人情報の参照が可能な事務室等における入退室管理に関する規程
・マニュアル類の文書管理に関する規程　等

【運用手順等】
・情報媒体紛失時の手順等
・情報破棄の手順等
・非常時における BCP（事業継続計画）に関する運用手順等
・非常時におけるアクセス管理の対応手順等（非常時用のユーザアカウントの取扱い手順を含む）

（４） 運用報告関係【関連する第 3 章の記述項目：3-1(最)3.、5.(h)(i)、3-3(最)4.、3-5(最)3..、3-6(最)5.、8.、3-6(推)2.、4.、3-12(最)(5).、3-12【ネットワークを通じて医療機関等の外部に保存する場合】(最) (3)、推奨、3-14【ネットワークを通じて医療機関等の外部に保存する場合】(最)2.、(推)1.、3-17】

ASP・SaaS 事業者は、サービス提供における運用内容等につき報告する義務を負う。その報告範囲、内容、方法、頻度等について医療機関等と協議し、合意すること。また、両者が求めた場合には、合意結果を契約、SLA 等で明文化すること。具体的には、以下を含む報告について協議対象とすること。
・サービス提供に必要な保守業務の実施報告（書面による作業の事前承認及び事後承認を含む）
・リモートメンテナンスによる保守等の実施状況

・サービス提供に必要な保守業務を、医療機関施設内で行った場合の実施報告
・サービス仕様の情報開示等
・ソフトウェアのカスタマイズ部分に関する作業内容
・受託した情報の処理に必要なシステムの動作確認において、やむを得ず受託した個人情報を使用する場合の結果報告
・個人情報を含む機器・媒体等の管理状況
・サービス提供において受託する個人情報へのデータアクセスが可能な端末が設置されている部屋の入退出記録
・保守等の体制変更が生じた場合の変更内容及びこれに伴うアカウント削除の実施等
・自社外に情報を持ち出す際の持ち出し記録
・アクセス管理に関する運用報告（アクセス制限、記録、点検等）
・バックアップの保存に関する運用報告
・自社において実施した監査結果に関する報告（実施水準、公開する範囲・条件等）
・情報の破棄を実施した場合の破棄記録等（契約終了時を含む）
・苦情・質問等の受付実績

（５） ネットワーク等との責任分界の範囲【関連する第３章の記述項目：3-9(最)6.、8.】

下記の項目についての責任分界について医療機関等と協議し、その合意結果を契約、SLA 等で明文化すること。
・ASP・SaaS 事業者におけるネットワーク通信に対する責任範囲
・障害が起こった際の対処

（６） 患者に対する説明義務等【関連する第３章の記述項目:3-1(最)5.(g)、3-16(最)(2)5①】

ASP・SaaS 事業者は、医療機関等の管理者が患者に対して説明責任を果たす際に、助力として医療機関等に提供する以下の事項について医療機関等と協議し、合意すること。また、両者が求めた場合には、その合意結果を契約、SLA 等で明文化すること。
・医療機関等の管理者が患者等に説明し同意を得る際に、ASP・SaaS 事業者が行う情報提供、説明の範囲、内容、方法等
・医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な情報の提供範囲、内容、方法等の役割分担等

（７） 契約終了

① ASP・SaaS提供契約終了の事前通知【関連する第３章の記述項目：3-17.】

ASP・SaaS 事業者は、サービス提供契約終了の事前通知手続について医療機関等と協議し、その合意結果を契約、SLA 等で明文化すること。

また、事業者の都合によりサービス提供を終了する際に、事前通知の手続によることが困難な場合（会社更生法の適用時等）の対応内容等についても医療機関等と協議し、契約、SLA 等で明文化することが望ましい。

② ASP・SaaS提供契約終了における受託情報引き渡し【関連する第３章の記述項目：3-17.】

ASP・SaaS 事業者は、サービス提供契約終了時に、受託情報を医療機関等に引き渡す際のデータ形式、データ内容、関連する資料の範囲、条件等について、医療機関等と協議し、その合意結果を契約、SLA 等で明文化すること。

受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「5 情報の相互運用性と標準化について」に従うこととし、その内容を契約、SLA 等で明文化すること。

特に、引き渡すデータに暗号化が施されている場合の対応等については明確にすること。

４．２．２　医療情報サービス全般で合意すべき機能に関する対応内容

ASP・SaaS で提供する医療情報サービスにおいて、外部保存の有無に関わらず、医療機関等との合意を図るべきサービス機能について以下に示す。

（１） 技術的安全管理対策に関する対応内容【関連する第３章の記述項目：3-3(最)5.、10. 3-3(推)5】

技術的安全管理対策に関する対応内容として、以下について、提供する機能レベル、範囲、サービスレベル等について医療機関等と協議し、合意すること。また、両者が求めた場合には、合意結果を契約、SLA 等で明文化すること。

・医療機関等の利用者の職種、担当業務等の設定に応じたアクセス制御機能の提供
・ アクセスの記録に用いる同期の取れた時刻の提供
・ パスワードポリシーに基づくアカウント管理
・採用する認証手段・方式

なお、合意の内容については、情報セキュリティ対策ガイドライン及び本ガイドライン３．２．３に示す内容を満たすものであること。

（２） 無線LANに関する対応内容【関連する第３章の記述項目:3-3(最)11.、3-3(推)6.】

医療機関等が ASP・SaaS の利用に際して無線 LAN を利用する場合に、医療機関等の無線 LAN が必要なセキュリティ対策についての、事業者の役割、範囲等について合意することについて契約、SLA 等に含める（表３-３(最)11.、(推)6.参照 。

（３） 通信の安全性に関する対応内容【関連する第３章の記述項目：3-9(最)1.－2.、4.－5.、8.－10.、3-9(推)1.】

通信の安全性に関する対応内容として、以下について、提供する機能レベル、範囲、サービス品質等について医療機関等と協議し、合意すること。また、両者が求めた場合には、合意結果を契約、SLA 等で明文化すること。

・ネットワーク経路上での不正メッセージ挿入、ウイルス混入等の改ざん、パスワード盗聴、本文の盗聴を防止する対策
・通信の起点・終点識別のための認証
・ルータ等のネットワーク機器の安全性を確保する機能
・秘匿性確保のための適切な暗号化(電子政府推奨の暗号鍵による暗号化等)

・患者に情報を閲覧させる場合のアクセス制御、暗号化等
・医療機関等の利用者がリモートアクセスを行う際のセキュリティ対策（仮想デスクトップ等）

合意の内容については、情報セキュリティ対策ガイドライン及び本ガイドライン３．２．９に示す内容を満たすものであること。

（４） 法令で定められた記名・押印を電子署名で行うことに関する対応内容【関連する第３章の記述項目項目：3-10(最)1.－3.】

ASP・SaaS 事業者が医療機関等と協議し、合意する電子署名の方式は、保健医療福祉分野 PKI 認証局の発行する電子署名もしくはこれと同等の仕様（厚生労働省の定める準拠性監査基準を満たすもの）を含むものであること。

４．２．３　外部保存を行う医療情報サービスで合意すべき機能に関する対応内容

（１） 真正性確保に関する対応内容【関連する第３章の記述項目項目：3-12(最)(1)－(5)】

真正性確保に関する対応内容として、以下について、提供する機能レベル、範囲、サービス品質等について医療機関等と協議し、合意すること。また、両者が求めた場合には、合意結果を契約、SLA 等で明文化すること。

・電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合の作成者の識別及び認証(職務権限等に応じたアクセスコントロール、機器におけるアクセスコントロール等)
・電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合の利用記録の確定機能（記録確定前に確認できることが必要）
・臨床検査システム、医用画像ファイリングシステム等、特定装置もしくはシステムにより記録される場合の、ASP・SaaS 事業者の役割、範囲等
・更新履歴の保存
・代行操作の承認機能
・機器、ソフトウェアの利用者教育についての ASP・SaaS 事業者の役割、範囲等

合意の内容については、情報セキュリティ対策ガイドライン及び本ガイドライン３．３．２に示す内容を満たすものであること。

（２） 見読性確保に関する対応内容【関連する第３章の記述項目項目：3-13【保存する場所について共通する内容】(最)(2)、(4)、【医療機関等に保存する場合】(最) (1)－(3)，【ネットワークを通じて外部に保存する場合】(推)(1)、(2)、3-15(推)(1)】

見読性確保に関する対応内容として、以下について、提供する機能レベル、範囲、サービス品質等について医療機関等と協議し、合意すること。また、両者が求めた場合には、合意結果を契約、SLA 等で明文化すること。

・見読化手段の管理
・見読目的に応じた応答時間とスループット
・システム障害対策（冗長性確保等、バックアップ、外部出力機能等）
・障害等が生じた場合の稼動に関するサービスの品質
・緊急時の医療機関等における診療録等の見読性確保を支援する機能(例えば画面の印刷機能等)

・外部保存を受託する機関において、診療録等へのアクセスを禁止する機能

合意の内容については、情報セキュリティ対策ガイドライン及び本ガイドライン３．３．３に示す内容を満たすものであること

（３） 保存性確保に関する対応内容【関連する第３章の記述項目項目：3-14(推) (2)3.、(推) (3)1.、(4)【保存する場所について共通する内容】(最)(2)、(3)、(4)、【ネットワークを通じて医療機関等の外部に保存する場合】(最) (1)、(2), (推) (1)】

保存性確保に関する対応内容として、以下について、実施する対策や運用の範囲、サービス品質等について医療機関等と協議し、合意すること。また、両者が求めた場合には、合意結果を契約、SLA 等で明文化すること。

・バックアップデータの内容の改善防止措置
・検索表示、書面表示の速度等
・ディスク障害対策
・診療録等のデータ、及びマスターテーブルにおける標準化されたデータフォーマットの使用
・データ形式及び転送プロトコルのバージョン管理と継続性の確保
・回線や設備が劣化した際にこれらを更新する等の対策
・設備の互換性確保

合意の内容については、情報セキュリティ対策ガイドライン及び本ガイドライン３．３．４に示す内容を満たすものであること。

４．３ 契約、SLA等の合意における注意点

４．２で示した各項目について、契約、SLA 等により合意するに際して、以下の点を留意する必要がある。

４．３．１ サービスレベルとコストに見合った提案

医療情報の取扱いに際しては高い安全性が求められる。機微な個人情報を取り扱うため、高度のセキュリティ確保が求められるほか、診療の継続に支障を来たさないようにするための可用性等も求められる。

従って第一に ASP・SaaS 事業者は、情報セキュリティ対策ガイドライン及び本ガイドラインに示す対策及び対応内容を遵守しながらサービスを提供することが求められ、医療機関との協議により合意する契約、SLA 等の内容もこれをみたすものであることが必要である。

その上で、一定水準以上のサービス品質を実現しようとする場合は、医療機関等のリスクに対する考え方に従って、ASP・SaaS 事業者と医療機関等とで協議することが必要になる。その際に、ASP・SaaS 事業者は、IT 技術や情報セキュリティ対策の専門家として、医療機関等に対し、コストとサービスレベルのバランスがニーズに合う提案を行うことが求められる。

４．３．２　医療機関等との責任分界の明確化

ASP・SaaS の安全性を確保をするためには、事業者側の対応だけではなく、医療機関等においても適切な運用管理を行なうことが求められる。例えば、ASP・SaaS が堅牢なアクセス制御機能を持っていたとしても、医療機関側の利用者がパスワードを利用端末に貼っていたり、アカウントを複数で共有していたり、院内無線 LAN のセキュリティ対策を怠っていたりしたら、サービスの安全は守ることができない。

従って、ASP・SaaS 事業者は、医療機関等と契約、SLA 等について協議するにあたり、医療機関等の側における運用管理対応等も踏まえた形で、責任分界を定めることが必要である。これにより、事故が発生した場合等の ASP・SaaS 事業者と医療機関等との責任の分担が明確になり、事後の対応を円滑に行うことができる。

４．４ サービスレベルマネジメントの実践

締結された契約、SLA 等の内容については、締結後、一定のサイクルで見直すことが求められる。情報通信技術は日進月歩で進歩しており、情報セキュリティ対策等の内容によっては数年で陳腐化してしまうケースも想定される。

ASP・SaaS 事業者が提供するサービスのサービスレベルについても、PDCA サイクルに基づいてサービス運用状況を計測、分析、評価した上で、技術環境の変化等も踏まえながら、継続的な改善を行っていく必要がある。

サービスレベルマネジメントの実践にあたっては、医療機関等と ASP・SaaS 事業者が協力してこれに当たることが望ましい。特に、ASP・SaaS 事業者は、情報システムの専門家として、サービスレベルマネジメントの向上に主体的に取り組む姿勢が求められる。